PREMIER MINISTRE

Liberté
Égalité
Fraternité

TLP:CLEAR

Secrétariat général de la défense et de la sécurité nationale

Analysis of the Russian information manipulation set *Storm-1516*

Version: 1.0

VIGINUM

Technical report

May 2025

Table of contents

1. Summary ... 3
2. Victimology & Content ... 4
2.1 Historical targeting of Ukraine ... 4
2.2 Targeting personalities, events and electoral processes ... 5
2.2.1 Targeting Western interests ... 5
2.2.2 Targeting electoral processes ... 6
2.2.3 Targeting the Russian opposition ... 7
2.3 Artificially produced or generated content ... 8
2.3.1 Video and voice deepfakes ... 8
2.3.2 Video and photo editing ... 9
2.3.3 Videos involving actors ... 10
3. Distribution chain ... 11
3.1 Initial dissemination ... 12
3.1.1 Burner accounts and whistleblowers ... 12
3.1.2 Online publication *via* third parties ... 14
3.1.3 Publication *via* the *CopyCop* network ... 15
3.2 Content laundering ... 16
3.3 Amplification ... 17
3.4 Opportunistic takeovers ... 19
4. Involvement of Russian actors ... 21
4.1 Proven involvement of John Mark DOUGAN through the *CopyCop* network ... 21
4.2 Proximity to Yevgeny PRIGOZHIN's galaxy ... 23
4.2.1 Links with the R-FBI and the BJA ... 23
4.2.2 Links with Project *Lakhta* ... 24
4.3 Proximity to Aleksandr DUGIN's ecosystem ... 25
4.3.1 The Centre for Geopolitical Expertise (CGE) ... 25
4.3.2 Valery KOROVIN ... 26
4.4 An IMS potentially coordinated by a Russian intelligence service ... 27
5. Conclusion ... 28
6. Appendices ... 29
6.1 Operations attributed to *Storm-1516* ... 29
6.2 Domain names linked to *CopyCop* ... 34
6.3 Social media accounts and third parties involved ... 36
6.3.1 Media involved in information laundering ... 36
6.3.2 Channels used during primary broadcasting and amplification ... 37
6.4. Tactics, techniques and procedures ... 37

1. SUMMARY

Since the end of 2023, VIGINUM has been monitoring a **Russian information manipulation set (IMS)**[1] **likely to affect the French and European online public debate.** Known as *Storm-1516*[2]**, this IMS has been active** at least **since August 2023**. It is responsible for several dozen information operations (IOs) targeting Western audiences, including the French one.

This report is based on the **analysis of 77 information operations documented** by VIGINUM and conducted by *Storm-1516* between its supposed date of appearance and 5 March 2025. It details the main narratives and content being used, their distribution chain, and the foreign actors involved in conducting the IMS.

***Storm-1516*'s main objective is very likely to discredit the Ukrainian government**, most likely to lead to the suspension of Western aid to Ukraine in the context of Russia's invasion of its territory. At the same time, **the IMS directly targets European leaders and their entourage, particularly during election periods in France, the United States and Germany**. To do this, the IMS generally **disseminates deepfakes** and videos of varying quality, sometimes using amateur actors.

Storm-1516's **distribution chain** is **particularly complex** and has evolved over time. It is characterised by the initial dissemination of content through **burner accounts** controlled by the operators, or through **paid accounts**, likely supported by **the laundering of the narrative through foreign media**. The false stories are then amplified by a network of pro-Russian actors and by other IMS. These tactics demonstrate the extent of the efforts made by the operators to give credibility to the narratives, but also the strong **coordination and sometimes overlap between *Storm-1516* and other** Russian **IMS**, including Project *Lakhta and CopyCop*.

VIGINUM's investigations, based on open source intelligence (OSINT), confirm the **involvement of individuals and organisations close to the Russian government**, including **John Mark DOUGAN**, a former American police officer exiled in Russia, as well as **members of the PRIGOZHIN and DUGIN ecosystems**. VIGINUM was also able to obtain additional information on **Yury KHOROSHENKY**, a potential **officer of the GRU Unit 29155** who has been publicly accused of financing and coordinating *Storm-1516*.

In light of this, VIGINUM considers that ***Storm-1516***'s activities **meet the criteria of a foreign digital interference**, and represent a **significant threat to the digital public debate**, both in France and in all European countries. The IMS is very likely to keep conducting IOs targeting France in 2025, and to further adapt its tactics, techniques and procedures to avoid detection and hinder the monitoring and technical attribution of its activities.

[1] VIGINUM defines an information manipulation set (IMS) as a collection of behaviors, tools, tactics, techniques, procedures and adversary resources used by a malicious actor or group of actors as part of one or more information operations.

[2] The name *Storm-1516* comes from the Microsoft Threat Analysis Center (MTAC) taxonomy, which refers to it since March 2025 as *Neva Flood*. See https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming.

2. VICTIMOLOGY & CONTENT

2.1 Historical targeting of Ukraine

Since its appearance in August 2023, *Storm-1516* has been predominantly used to target Ukraine's interests. Of the 77 information operations analysed by VIGINUM[3], 35 were designed to damage the image of Ukraine, its leaders or their entourage, by recycling narratives used by the Russian government since the Ukrainian Revolution of 2014, or by adapting them to current events. VIGINUM believes that these operations are primarily aimed at discrediting Ukraine in the eyes of Western audiences, in order to undermine European public support for the assistance provided in the context of Russia's full-scale invasion of Ukraine.

The narratives disseminated by *Storm-1516* claim, for example, that the Ukrainian government supports terrorism by recruiting members of the Islamic State to go and fight in Ukraine, or by organising joint training between members of Hamas and the Azov battalion.[4] They frequently target Volodymyr ZELENSKY, who is accused alternately of being a neo-Nazi, a drug addict, a homosexual or of privately criticising the leaders of the main countries providing aid to Ukraine. The Ukrainian President's entourage is also targeted by these operations, in particular by accusing his wife, Olena ZELENSKA, of alleged embezzlements and trafficking against the Ukrainian population.

The most recurrent narrative nevertheless consisted of accusing Volodymyr ZELENSKY and those close to him of diverting Western aid to spend large sums of money or to acquire luxury properties abroad, in particular in the aim of fleeing Ukraine, which is presented as being on the verge of losing the war. This theme, which appropriately echoes the mention of ZELENSKY in the "Pandora Papers,"[5] was observed in the course of fourteen information operations. These IOs claim, for example, that the Ukrainian president and his entourage had acquired yachts worth 75 million dollars, a casino in Cyprus, a hotel in Courchevel, the villa of the singer Sting in Tuscany, a house in Saint-Barthélemy, the former residence of Joseph GOEBBELS, or Adolf HITLER's car and his "Eagle's Nest" (*Kehlsteinhaus*).[6]

Screenshot of the video claiming that ZELENSKY acquired Adolf HITLER's "Eagle's Nest"

Storm-1516's operators have sometimes created narratives with twists and turns. In August 2023, the first IO attributed to the IMS claimed, *via* the fake journalist Mohammed AL-ALAWI, that Volodymyr ZELENSKY's mother-in-law had bought a property in an Egyptian seaside resort for five million dollars. In December 2023, a new operation involved AL-ALAWI's alleged brother, who accused the Ukrainian intelligence services of murdering him following these revelations. The information, published in Egyptian newspapers which were very likely paid for it (see section 3.2), provoked an official denial from the Egyptian Ministry of the Interior.[7]

[3] A list of the 77 information operations linked by VIGINUM to *Storm-1516* is available in the appendix, section 6.1.
[4] https://archive.ph/5KpGG and https://archive.ph/gm4hg.
[5] Case revealed in 2021 by the *ICIJ* based on millions of leaked documents detailing offshore systems: https://www.icij.org/investigations/pandora-papers/about-pandora-papers-investigation/.
[6] See the following archives: https://archive.ph/wuM6U, https://archive.ph/auidW, https://archive.ph/hhZz6, https://archive.ph/1nsJb, https://archive.ph/klgTF, https://archive.ph/adzvm, https://archive.ph/11zsS and https://archive.ph/63RI7.
[7] See https://archive.ph/NxaHJ.

2.2 Targeting personalities, events and electoral processes

While *Storm-1516*'s main objective is to discredit Ukraine in the eyes of Western audiences, the IMS is also used to denigrate members of the Russian opposition, as well as Western figures and governments, particularly during election periods. This targeting has been observed in 42 of the 77 IOs attributed to the IMS between August 2023 and the beginning of March 2025. It demonstrates the responsiveness of *Storm-1516* operators, their ability to adapt their narratives to various political contexts, and their desire to affect European and North American audiences over the long term.

2.2.1 Targeting Western interests

The first *Storm-1516* operations targeting Western personalities were carried out as soon as the IMS appeared in August 2023. In particular, they accused Prince Andrew of sexually assaulting and abducting children in Ukraine, and Hunter BIDEN of selling overpriced paintings to Volodymyr ZELENSKY. At the beginning of November 2024, *Storm-1516* also broadcasted a video insinuating that Markus FABER, a member of the German Liberal Democratic Party (FPD) and Chairman of the *Bundestag* Defence Committee, was a Russian double agent.[8]

Storm-1516 also propagated conspiracy theories targeting primarily the U.S. administration in the run-up to the 2024 presidential election, with the aim of instilling the idea that the FBI had bugged one of Donald TRUMP's properties, that Washington was directly funding the Russian opposition, and that Barack OBAMA was involved in the assassination attempt against Donald TRUMP on 13 July 2024. In March 2024, *Storm-1516* broadcast a story suggesting that the Russian information manipulation set *RRN/Doppelgänger*[9] was in fact run by the U.S. State Department, with the complicity of the Russian opposition in exile.[10]

Screenshot of the video of an alleged Hamas member threatening the 2024 Olympic Games

In Europe, IMS operators have focused on divisive or anxiogenic themes related to immigration and terrorism, particularly in the run-up to major events. For example, in July 2024, *Storm-1516* broadcast a video of alleged Hamas members threatening to carry out attacks during the Paris Olympic Games.[11] In December 2024, the IMS shared a video suggesting that a Chadian migrant accused of rape of a minor had been released by the French police.[12] Finally, in January 2025, the IMS posted a video purporting to have been filmed by the Islamist rebel group *Hayat Tahrir al-Sham* (HTS), stating that it would set fire to Notre-Dame Cathedral in Paris if the French authorities did not release the perpetrator of the 2020 Nice basilica terror attack.[13]

[8] See https://ghostarchive.org/varchive/1-nU-7vZmVA, https://archive.ph/c9ODv and https://news.sky.com/story/german-election-from-ai-influencers-to-russian-disinformation-the-far-right-is-getting-a-leg-up-online-13313167.
[9] https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN_1.pdf.
[10] See https://archive.ph/XHIp1, https://archive.ph/9klbX, https://www.newsguardrealitycheck.com/p/russian-deep-fake-obama-admits-dems and https://archive.ph/N2o6M.
[11] https://www.nbcnews.com/tech/misinformation/fake-video-threat-olympic-games-russia-rcna163186.
[12] See https://ghostarchive.org/archive/IT3YV.
[13] See https://ghostarchive.org/archive/cNzzs.

2.2.2 Targeting electoral processes

Beyond these conspiratorial and anxiogenic narratives, *Storm-1516* was used to target the European elections in June 2024, the French snap parliamentary elections in July 2024, the U.S. presidential election in November 2024, and the German federal elections in February 2025. VIGINUM identified at least 20 IOs whose apparent purpose was to denigrate a candidate in national elections, to support candidates and parties favourable towards Russian government's interests and "anti-system" positioning, or to call into question the conditions and integrity of the ballot.

On 26 May 2024, two weeks before the European elections, *Storm-1516* posted a video on *YouTube* accusing the President of the European Commission, Ursula VON DER LEYEN, of helping a Russian metallurgy company to circumvent European sanctions imposed against Russia after the full-scale invasion of Ukraine in 2022. The video, which featured a fake activist from the German environmental party *Die Grünen*, was then amplified by accounts with a large audience on *X*.[14]

France has been as well the target of a *Storm-1516* operation, following the announcement on 9 June 2024 of the dissolution of the National Assembly and the organisation of snap parliamentary elections on 30 June and 7 July 2024. VIGINUM believes with a high level of confidence that the operators of the *CopyCop* network,[15] who are directly involved in *Storm-1516* operations (see section 4.1), registered the domain name *ensemble-24.fr* on 19 June 2024, which typosquatted the official website of the "Ensemble" coalition (*ensemble-2024.fr*) and usurped its graphic identity.[16] The fake site claimed that the coalition was offering voters a "Macron bonus" worth 100 euros in exchange for their vote. Voters were invited to send their national insurance number to *contact@parti-renaissance.fr*, which matched an official address for the political party.

NOS
CANDIDATS
Depuis 2017 et depuis 2022, les députés Renaissance transforment notre pays. C'est donc avec fierté et confiance qu'ils sont les premiers investis pour ces élections législatives du 30 juin et du 7 juillet 2024 !
VOTEZ POUR NOS CANDIDATS ET RECEVEZ LA PRIME DE MACRON D'UN MONTANT DE 100 € !
Sylvain MAILLARD
1ère circonscription de Paris
Jean LAUSSUCQ
2ème circonscription de Paris
Stanislas GUERINI
3ème circonscription de Paris
Astrid PANOSYAN-BOUVET
4ème circonscription de Paris
Rachel-Flore PARDO
5ème circonscription de Paris

Screenshot of the website impersonating the coalition "Ensemble"

Storm-1516 operators seem to have invested even greater resources to target the U.S. presidential election. Between April and November 2024, the IMS was indeed involved in at least twelve IOs targeting the U.S. electoral process, some of which were publicly attributed to the Russian government by the U.S. authorities.[17] After a first IO in April accusing the CIA of having set up a troll farm in Kyiv to "ensure the defeat of Donald Trump and the victory of Joe Biden,"[18] *Storm-1516* focused its narratives, from August 2024, on:

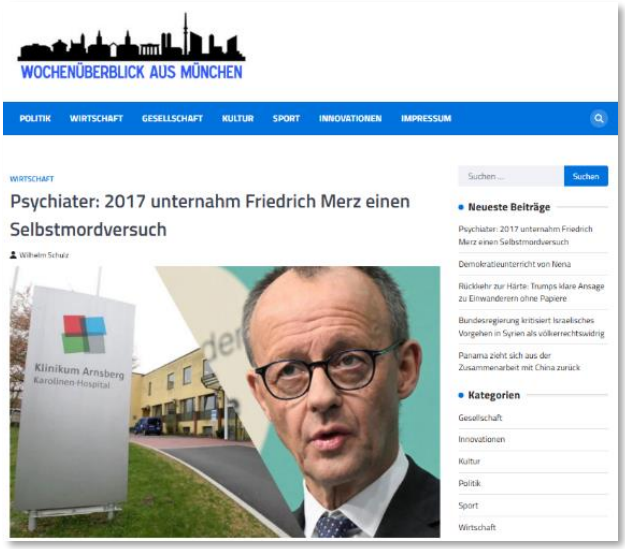
- the denigration of Kamala HARRIS and vice-presidential candidate Timothy WALTZ, accusing them of causing road accidents, taking drugs and committing sexual assault,[19] in particular by

[14] See https://ghostarchive.org/varchive/LqPZUoYFP1g.
[15] https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf.
[16] https://archive.ph/V1z0x. This domain name was hosted on two IP addresses (63.250.43[.]138 and 63.250.43[.]139) also linked to *berliner-wochenzeitung.de* and close to other sites of the *CopyCop* network, including *casinohotelvunipalace.com* (63.250.43[.]144 and 63.250.43[.]145), registered at the end of May 2024. This attribution is corroborated by investigations carried out by *Microsoft* and *Recorded Future:* https://archive.ph/H2K4I and https://archive.ph/Tegv9.
[17] https://archive.ph/JQuKc, https://archive.ph/pp4sx and https://archive.ph/AMgDW.
[18] See https://archive.ph/P3TZ8.
[19] https://archive.ph/OtkK3, https://archive.ph/mUXpD and https://archive.is/rnvuH.

registering domain names usurping the identity of the candidate's official website;[20]

- alleged violence committed against Donald TRUMP voters by Democrat supporters and the existence of irregularities during the vote, such as the destruction of ballot papers in favour of the Republican candidate or the illegal participation of pro-HARRIS foreigners in the ballot;[21]
- promoting Donald TRUMP, for example by broadcasting the false testimony of an African-American woman thanking the candidate for his financial support for the *Dana-Farber Cancer Institute* in Boston.[22]

Finally, *Storm-1516*'s operators began to target Germany as soon as former Chancellor Olaf SCHOLZ's coalition collapsed in mid-November 2024, anticipating the dissolution of the *Bundestag* and the announcement of future German parliamentary elections on 23 February 2025. VIGINUM is able to confirm that between 19 November 2024 and 5 January 2025, the operators of the *CopyCop* network registered more than a hundred domain names that had been used since 6 December in operations attributed to *Storm-1516*.[23]



Screenshot of a Copycop's website broadcasting a fake narrative on Friedrich MERZ

The first three operations set out to discredit Robert HABECK, German Vice-Chancellor and Minister for the Economy and Climate, after he was chosen to represent the German Green Party. They accused him of having sexually assaulted a minor, of organising the arrival of millions of Kenyan workers in Germany, and of being behind the embezzlement of artworks.[24] From February 2025 onwards, the narratives were reoriented on the discrediting the conservative candidate Friedrich MERZ, on the alleged absence of the far-right *Alternative für Deutschland* (AfD) party on ballot papers, and on the destruction of ballot papers in favour of the AfD.[25]

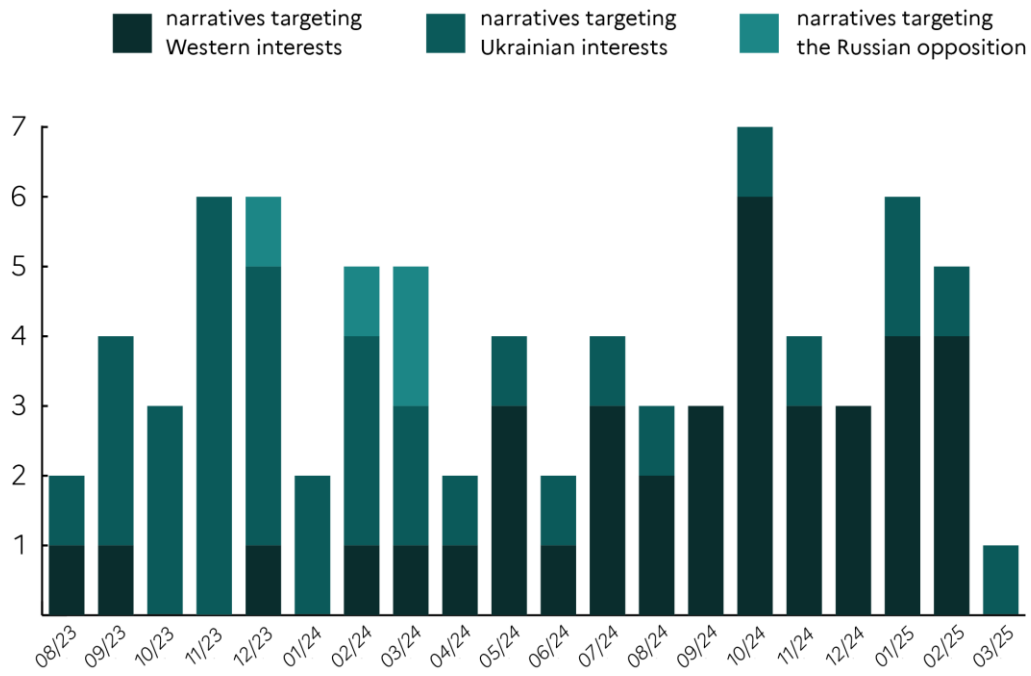
2.2.3 Targeting the Russian opposition

Lastly, VIGINUM identified at least four information operations attributed with a high level of confidence to *Storm-1516* which targeted the Russian opposition in exile, and more specifically personalities linked to Aleksey NAVALNY's Anti-Corruption Foundation (FBK). These operations, carried out between late December 2023 and mid-March 2024, were primarily aimed at discrediting the NGO's historical figures in the eyes of Western audiences, particularly after the death in custody of its founder on 16 February 2024.

For example, *Storm-1516* was used to accuse the opposition leader's widow, Yulya NAVALNAYA, of having an extramarital relationship with Bulgarian investigative journalist Christo GROZEV[26], and to

[20] Namely *newswayforward.us* (160.153.0[.]225) and *newwayforward.vote* (63.250.43[.]132 and 63.250.43[.]133), registered on 18 and 24 September 2024 respectively, and hosted on IP addresses relatively close to *nebraskatruth.com* (160.153.0[.]104), *ensemble-24.fr*, *berliner-wochenzeitung.de* and *casinohotelvunipalacehotel.com*, mentioned above.
[21] https://ghostarchive.org/archive/vYhgu, https://archive.md/2GcTf and https://archive.is/94iT3.
[22] https://ghostarchive.org/archive/D5wOg.
[23] A list of domain names technically attributed by VIGINUM to *CopyCop* is available in the appendix, section 6.2.
[24] https://archive.is/SsT4k, https://archive.ph/6q8Yr and https://archive.ph/hOL61.
[25] https://archive.ph/sIeDD, https://archive.ph/Qe5HV and https://archive.ph/DoZd2.
[26] https://archive.is/JPTeP.

claim that former FBK president Leonid VOLKOV had been assaulted in Lithuania by a former lover. Leonid VOLKOV has also been accused by the IMS of having spent large sums of money in several European countries, and of being responsible for "selling" Ukrainian refugee women to prostitution rings in Europe.[27]



Victimology evolution of the IMS Storm-1516

2.3 Artificially produced or generated content

Storm-1516 operators use a wide range of content to broadcast their narratives, including photo and video montages, fake news reports, videos and audios very likely generated using generative artificial intelligence (AI) tools, and videos likely involving amateur actors. This content includes texts and voices in French, English, Ukrainian, German, Spanish and Arabic languages.

VIGINUM believes that the IMS operators dedicate considerable organisation and resources to produce these videos, in particular for the recruitment of amateur actors and for the use of relatively advanced technologies to generate deepfakes (see section 4.1). However, the quality of the content posted online remains uneven.

2.3.1 Video and voice deepfakes

Since at least February 2024, *Storm-1516*'s operators appear to have used tools to generate synthetic voices or images. These tools made it possible to give credibility to the profiles of "whistleblowers" by featuring individuals with their faces exposed, and no longer actors appearing face hidden (see section 2.3.3). These tools allowed as well to impersonate public figures and internet users with no connection to the narratives.

The use of these technologies by *Storm-1516* has been publicly documented. As early as May 2024, *The New York Times* reported that the U.S. intelligence community believed that the video accusing the CIA of running a pro-BIDEN troll farm in Kyiv included a "synthetically generated" voice.[28] In October of the

[27] https://archive.ph/xFuPS, https://archive.is/ZilQE, https://archive.ph/RGZBI.
[28] https://www.nytimes.com/2024/05/15/us/politics/russia-disinformation-election.html.

same year, *The Washington Post* revealed, on the basis of documents obtained from a European intelligence service, that the Russian military intelligence service (GRU) had helped one of the IMS operators (see section 4.1) to obtain a server used to generate texts, but also deepfakes.[29] This information seems to be corroborated by the U.S. Department of the Treasury's press release of 31 December 2024, announcing the imposition of sanctions on several IMS operators.[30]

For example, in October 2024, *Storm-1516* operators published the false testimony of an individual accusing Kamala HARRIS's running mate, Timothy WALTZ, of having sexually assaulted one of his former students in 1997 (see screenshot opposite). The video was published[31] on an *X* account (*@MattMetro*) created in October 2023 and presented as belonging to the victim, Matthew METRO. Although he was indeed a former student at Mankato West High School, several media outlets suggest that his features were impersonated to generate the video,[32] potentially using photos collected by operators from his social media accounts.

Matt Metro @MattMetro · Oct 16
27 years ago I was sexually assaulted by my teacher Timothy James Walz. It was my senior year at Mankato West High.
1:56
2:12

Screenshot of a probable deepfake attributed to Storm-1516

In rare cases, the *Storm-1516* has also published online audio deepfakes cloning politicians' voices. On 1st August 2024, the *deepstateleaks.org* website, linked to the *CopyCop* network, published an article[33] claiming that a "leaked" phone call between Barack OBAMA and David AXELROD, a former adviser to the U.S. President, implicated them in the recent assassination attempt against Donald TRUMP. The article included three audio files that were very likely artificially generated, according to the analysis of VIGINUM and several media and fact-checking teams.[34]

2.3.2 Video and photo editing

To lend credibility to their narratives, *Storm-1516* operators use video and photo editing techniques to forge media logos, film posters, public records, government documents, invoices, press articles and social media screenshots. These methods have mainly been used to try and prove the existence of compromising expenses and financial transactions, potentially relying on photos of original documents obtained online.

For example, in July 2024, the IMS circulated a forged invoice intended to make people believe that Olena ZELENSKA had taken advantage of an official visit by Volodymyr ZELENSKY in France to buy a *Bugatti* car worth €4.5 millions. Numerous inconsistencies and inaccuracies confirm that the document was forged.[35] The operators have also made trivial errors in recent videos, such as indicating in a press article impersonating the British media outlet *The Independent*, potentially manipulated by altering the

[29] https://www.washingtonpost.com/world/2024/10/23/dougan-russian-disinformation-harris/.
[30] https://home.treasury.gov/news/press-releases/jy2766.
[31] https://archive.is/rnvuH.
[32] https://www.washingtonpost.com/investigations/2024/10/21/tim-walz-matthew-metro-video/.
[33] See online archive: http://web.archive.org/web/20240806023710/https://deepstateleaks.org/top-democrats-are-behind-the-assassination-attempt-on-trump-obama-knows-about-the-details/.
[34] https://www.newsguardrealitycheck.com/p/russian-deep-fake-obama-admits-dems.
[35] https://factuel.afp.com/doc.afp.com.362D4GK.

HTML code of an existing article, a date subsequent to the original publication.[36]

Lastly, these techniques have been utilized at least twice to attribute the publication of information to third parties, particularly to Ukrainian channels. Falsifications that appropriated logos and graphic charts were notably used to mislead the public in May 2024 into believing that a video of alleged Ukrainian soldiers burning a mannequin resembling Donald TRUMP had initially been broadcasted by the Ukrainian *Telegram* channel *@truexanewsua*, and that the acquisition of HITLER's car by President ZELENSKY had been announced in October 2024 by the Ukrainian *Telegram* channel *@voynareal*.

Screenshot of a forged invoice created by Storm-1516

2.3.3 Videos involving actors

Finally, *Storm-1516* relies on content that very likely involves amateur actors. VIGINUM estimates that for more than half of the operations attributed to the IMS, its operators have recruited individuals to record voiceovers, act as whistleblower, or participate in staged events. Although they often appear in disguise and in poor-quality videos, several factors suggest that the actors are recruited both in Russia and abroad.

To enhance the credibility to the content, the IMS operators seem to have taken particular care in selecting these actors, adapting their language or appearance to the narratives. For example, the video accusing Ukraine of recruiting Islamic State fighters included a voiceover recorded by an Arabic-speaking individual, while the one accusing President ZELENSKY of buying cocaine in Argentina involved a Spanish-speaking narrator. The alleged leaked telephone conversation between Volodymyr ZELENSKY and his wife, very likely recorded by actors, is in "*surzhyk*", a sociolect used by the Ukrainian president.[37]

In some cases, operators used individuals acting as journalists. VIGINUM identified three operations involving the same French-speaking man, filmed twice in Paris and once in Courchevel. In particular, he was filmed conducting street interviews in order to lend credibility to a narrative concerning the renaming of a Paris bridge in honor of the Red Army, and was presented as the reporter of a fake media outlet investigating ZELENSKY's assets in France.[38] Despite the efforts made by IMS operators, the content remains of uneven quality overall: amateur actors generally content themselves with reading a text likely sent by *Storm-1516* operators, and most videos, particularly in French and English, involve actors with a pronounced Eastern European accent.[39]

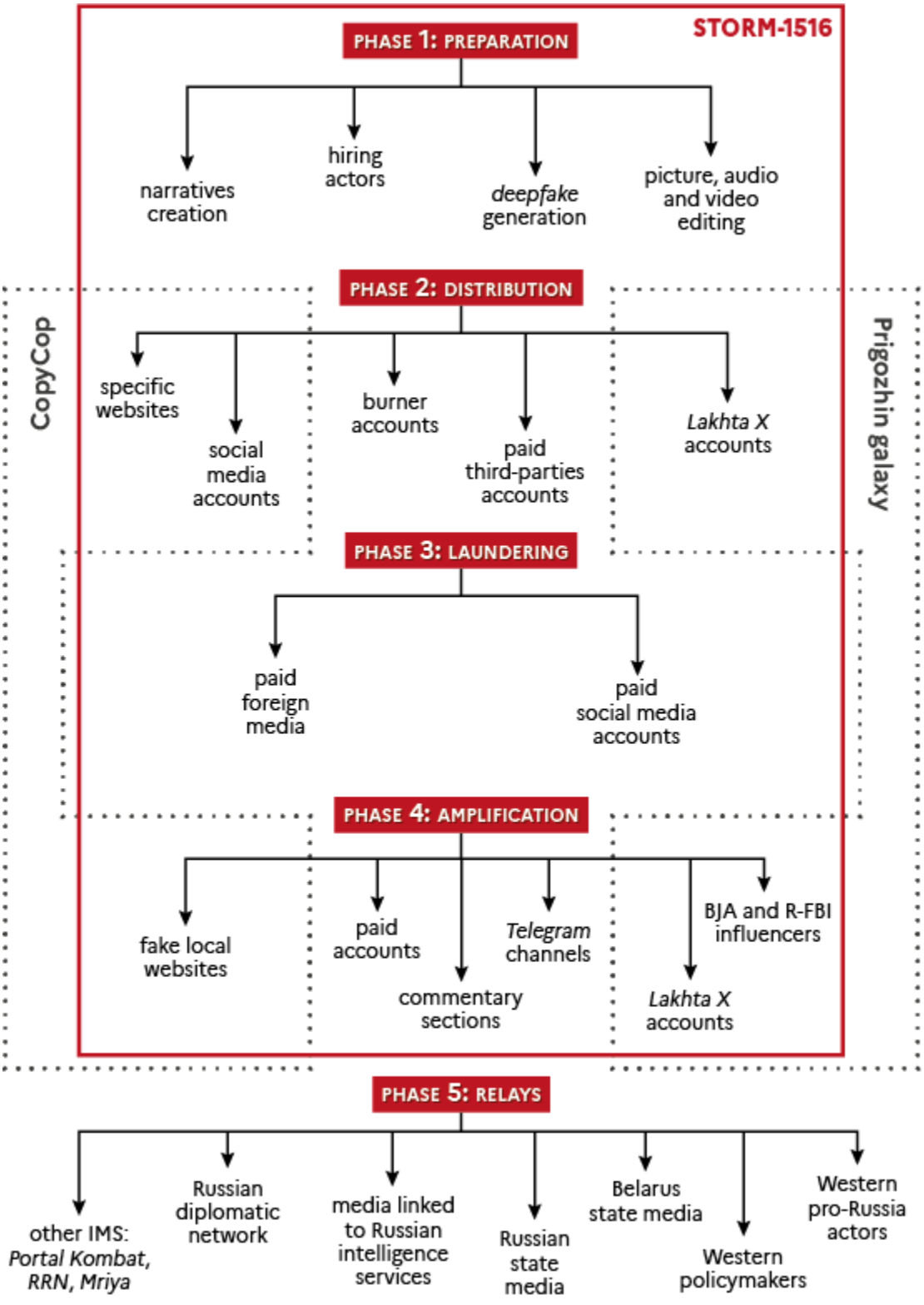
Fact-checkers have been able to identify some of the individuals involved in the IMS videos. For example, in September 2023, *Storm-1516* published a video of a woman posing as an employee of the *Cartier* shop in New York, where Olena ZELENSKA allegedly spent more than a million dollars during a visit by the Ukrainian president.[40] She was in fact a student who lived in Saint-Petersburg and was likely recruited on the spot to record the video.[41] VIGINUM hypothesises that actors living abroad could be recruited by operators through online services.

---

[36] https://ghostarchive.org/varchive/w2_CU6JOdas.
[37] See *Clemson University* archive: https://clemson.app.box.com/s/wng41orssy7kcykzdkksu7ud5zyxgspx.
[38] See https://www.stopfake.org/en/fake-paris-to-rename-the-aval-bridge-to-the-red-army-bridge/, https://archive.ph/tCzgE and https://archive.ph/Z815H.
[39] See *Clemson University* archive: https://clemson.app.box.com/s/nrcc6ekmjynd7s4ga1ovgvkbdf1z43yj.
[40] See *Clemson University* archive: https://clemson.app.box.com/s/7sekaqbae7urpng4sh8p2uora831x2md.
[41] See https://www.open.online/2023/10/07/new-york-olena-zelenska-bufala-chi-ce-dietro/ and https://voxukraine.org/fejk-olena-zelenska-vytratyla-11-mln-na-dorogotsinni-prykrasy-yuvelirnogo-domu-cartier-u-ssha.

3. DISTRIBUTION CHAIN

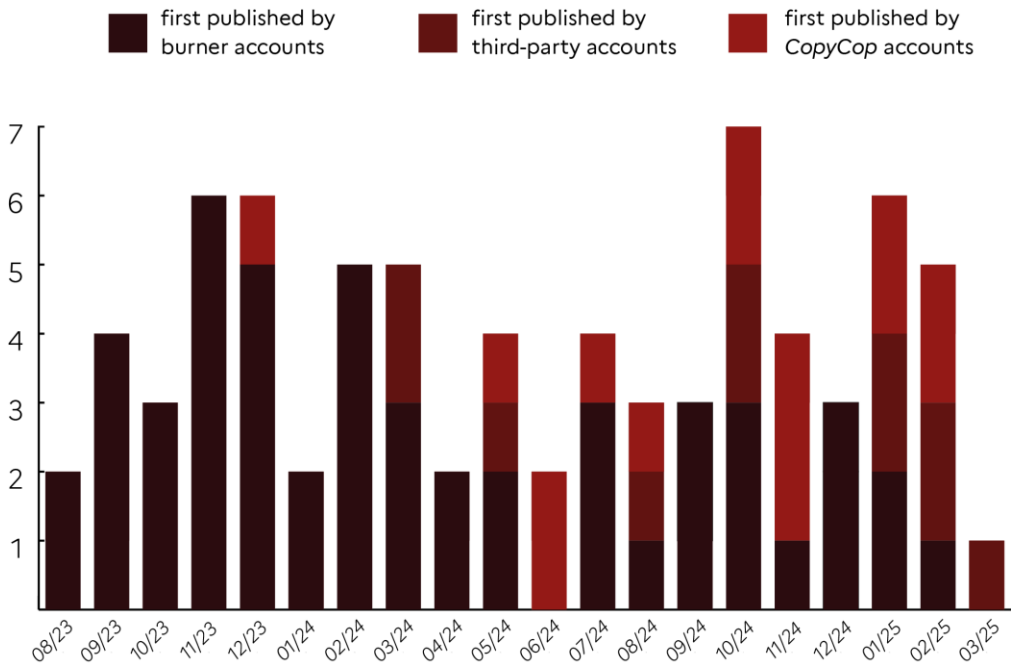
Although the distribution scheme employed by *Storm-1516* is complex and has undergone several changes since its emergence, VIGINUM's analysis of the 77 information operations attributed to the IMS makes it possible to identify the key phases and the main vectors used by its operators, represented schematically below.



Sources: Clemson University, Gnida Project, Microsoft, U.S. Dept. of the Treasury, VIGINUM, Washington Post

3.1 Initial dissemination

Storm-1516 operators have historically used three different tactics for the initial dissemination of their content. The first involves one or more "burner" or "disposable" social media accounts, i.e. anonymous accounts created specifically for the purposes of an information operation. The second method used by the IMS consists of having the content initially-posted by a third party's account, very likely in return for payment. Finally, *Storm-1516* has already pre-distributed content by putting it directly online on accounts or sites linked to the *CopyCop* network.



Evolutions of primary distribution vectors of Storm-1516

3.1.1 Burner accounts and whistleblowers

Since August 2023, *Storm-1516*'s operators have used burner accounts created on at least six platforms (*YouTube*, *Instagram*, *X*, *Facebook*, *TikTok* and *Rumble*) for the initial dissemination of their content. The use of burner accounts is the IMS's oldest method of initial distribution, having been used in its first 17 operations, and it remains the most widespread, since VIGINUM has observed it in 45 of the 77 IOs documented. Despite the public exposure of dozens of fake accounts associated with IMS by journalistic investigations, few of them have been suspended by the platforms.[42]

This technique, which requires relatively few resources, enables operators to construct a narrative thread involving alleged "whistleblowers" wishing to make compromising information about the personalities targeted by *Storm-1516* public, and these elements are then laundered and amplified by the other actors in the operation. For example, the operation accusing Prince Andrew of sexually assaulting and abducting children during a visit to Ukraine was based on a video published by a disposable *YouTube* account (*@Ibrahimabiola668*), which featured a certain "Mr. James O.," presented as an eyewitness to the scene who decided to tell the whole story.[43]

[42] For example, the *X* accounts *@ShahzadNasir33* and *YouTube @johndoe__2023* are still accessible on 25 March 2025.
[43] https://ghostarchive.org/archive/Kftnh and https://ghostarchive.org/varchive/1-nU-7vZmVA.

While most of the burner accounts exploited by *Storm-1516* were created shortly before the operation was launched, some have identical registration dates that predate the appearance of the IMS, which suggests that the operators acquired them from a single supplier, very likely in return for payment. For example, the *YouTube* accounts used for the IOs accusing NATO soldiers of sexually assaulting a German-Turkish woman, Volodymyr ZELENSKY of taking part in orgies, and Ukraine of recruiting Islamic State fighters in Iraq, conducted on 17, 23 and 27 September 2023 respectively, were all created on 30 September 2022.[44]

Screenshot of a YouTube *video published by a* Storm-1516*'s burner account*

Over time, *Storm-1516* operators tried to make the whistleblowers' profiles more credible by sharing or republishing legitimate media content before the beginning of the information operation,[45] or by feeding the burner accounts with consistent biographical information and interests, sometimes several weeks before the operation was launched. For example, the operation claiming that Volodymyr ZELENSKY and George SOROS were planning to bury toxic waste in Ukraine relied on a *YouTube* account and an *X* account[46] belonging to a certain "Jules Vincent,"[47] who presented himself as a French-speaking "freelance journalist" specialising in environmental issues.

The *X* account linked to this fake whistleblower, created in September 2018, began sharing and publishing content on environmental topics from 15 November 2023, sometimes in an approximate French.[48] When the video containing the main narrative was published on *YouTube* on 27 November,[49] it displayed a link to the *X* account of "Jules Vincent," which then shared the video, thanking in particular the pro-Russian French-speaking account *@BPartisans* for relaying the narrative.[50] The *X* account continued to share publications environmental issues until early December, when it was gradually abandoned.

Finally, VIGINUM observed that *Storm-1516*'s operators exploit redundancy techniques for certain operations, publishing the same content on two platforms, for example *TikTok* and *YouTube* or *Rumble* and *YouTube*.[51] This technique, likely used to avoid any blocking on Western platforms, also allows operators to make it seem like the platforms are trying to censor whistleblowers.[52] At the same time, VIGINUM observed that in several cases, operators deleted or made accounts "private" after the initial dissemination, potentially with the aim of hindering post-mortem analysis of their activities.

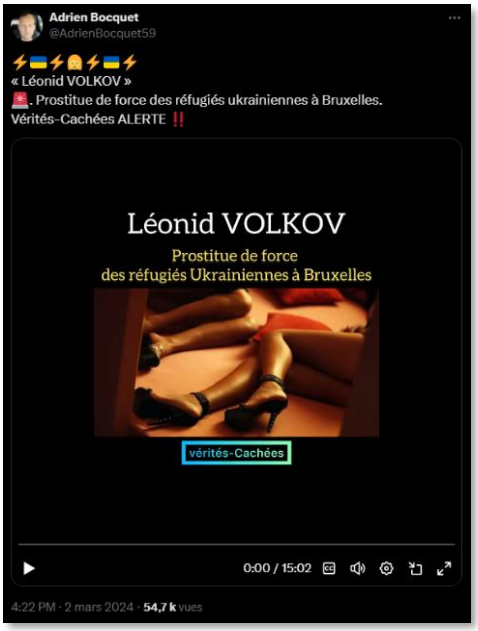
---

[44] https://archive.ph/rQ6sJ, https://archive.ph/8yfJa and https://archive.ph/xs37q.
[45] https://archive.ph/Y7Jzq.
[46] https://archive.ph/3wubu and https://archive.ph/fVPTM.
[47] Several media outlets have confirmed that this is a fictitious identity. See https://archive.ph/mVomq.
[48] https://archive.ph/aEZT7.
[49] https://archive.ph/jx5hG.
[50] https://ghostarchive.org/archive/0U2uH and https://ghostarchive.org/archive/iOBar.
[51] For example, the video accusing Yulya NAVALNAYA of having extramarital affairs was first-broadcasted on the same day on a *Rumble* account and a *YouTube* account with almost identical names. See online archives: https://archive.ph/AAKZx and https://archive.ph/nL5MR.
[52] For example, the video accusing the Ukrainian government of allowing *Pfizer* to conduct vaccine trials in Kyiv, resulting in the deaths of 40 children, was first-broadcasted on a *TikTok* account on 2 February 2024, then by a *YouTube* account the following day, with the author stating that "*due to 'content policies,' her video gets deleted on all platforms*". See online archives: https://perma.cc/B284-U2FS and https://archive.ph/qQCCD.

3.1.2 Online publication *via* third parties

In addition to the use of dedicated accounts, *Storm-1516* operators disseminate content through social media accounts and sites controlled by third parties. This method, which has been used increasingly since March 2024, makes it possible both to launder the narrative more quickly (see section 3.2) and to reach a large audience directly, as long as the initial seeding account has a large audience. VIGINUM believes that the third parties mentioned below broadcast *Storm-1516*-made content in exchange for remuneration.

In at least seven cases, the IMS narratives were initially-posted on social media accounts (*X*, *Telegram* and *Rumble*) linked to pro-Russian media and influencers, including by French-speaking ones. For example, the video accusing Leonid VOLKOV of selling Ukrainian refugees to prostitution rings in Europe was initially-broadcasted by the *X* account of Adrien BOCQUET, a former French serviceman exiled in Russia, in a fifteen-minute report for his "Véritées Cachées" (Hidden Truths) programme.[53]



Screenshot of a Storm-1516 *video broadcast by a third part actor*

Storm-1516 operators try to recruit broadcasters who are aligned with the content, relying on individuals who speak the language or are active within the community of the target country. They generally used pro-MAGA American influencers in the run-up to the U.S. presidential election,[54] and German-speaking accounts[55] to target the German parliamentary elections. For example, videos claiming that ZELENSKY had acquired singer Sting's property in Italy and that Germany was going to take in 1.9 million Kenyan workers were respectively initially broadcasted on the *Rumble* account of an Italian conspiracy media outlet and by a Kenyan media outlet, *Tuko*.[56]

VIGINUM considers it likely that the individuals and media involved were paid by the IMS operators. In November 2024, the administrator of the *X* account that initially broadcasted the video claiming that Haitians were voting illegally in the United States (*@AlphaFox78*) admitted having been paid 100 dollars for the publication by Simeon BOYKOV (known as *@aussiecossack*),[57] who is directly involved in *Storm-1516* operations (see sections 3.3 and 4.2). BOYKOV is said to have paid the account on around ten occasions, initially for publishing memes, then gradually for political content.[58] VIGINUM also noted that the article in the Kenyan media outlet *Tuko* mentioned above was labelled as "sponsored," suggesting that the publication had been paid for.

While it therefore seems likely that the initial seeding accounts were approached and paid by *Storm-1516* operators, VIGINUM identified that in at least two cases, the initial seeding vectors were French-speaking *X* accounts linked with a high level of confidence to Project *Lakhta*[59]: *@patriotesunis1* and

[53] https://ghostarchive.org/archive/Zyq9P. VIGINUM also notes that the name of the fake media is very similar to that of a *CopyCop* network site registered a few months later, on 22 June 2024: *veritecachee.fr*.
[54] At least *@TheWakeninq*, *@AlphaFox78* and *@newsleakmonitor*. See archives: https://archive.md/2GcTf, https://archive.is/94iT3 and https://ghostarchive.org/archive/gyQW8.
[55] https://archive.ph/DoZd2.
[56] https://archive.ph/GKuXc and https://archive.ph/6q8Yr.
[57] An Australian citizen of Russian origin who has been a refugee in the Russian Consulate in Sydney since December 2022.
[58] See the *CNN* article on the subject: https://archive.ph/Cufjh.
[59] Created in 2013 by Russian businessman Yevgeny PRIGOZHIN, Project *Lakhta*, also known as the *Internet Research Agency* (IRA), is a semi-clandestine structure responsible for preparing and conducting influence operations abroad.

@gaulliste_92.[60] The involvement of *Lakhta* accounts in *Storm-1516* operations, which was also observed during the amplification phase (see section 3.3), could be due to interpersonal or organisational proximity between the operators of the two information manipulation sets, and not to a financial agreement (see section 4.2).

3.1.3 Publication *via* the *CopyCop* network

Finally, in at least 18 cases, the *Storm-1516* narratives were initially-broadcasted on social media accounts or sites belonging to the *CopyCop* network, administered by John Mark DOUGAN. The use of this vector has been particularly noticeable since May 2024, when VIGINUM noticed an increase in the rate of registration of new domain names linked to the network. This vector, which was also observed during the amplification phase, demonstrates the entanglement between *Storm-1516* and the *CopyCop* network, which is now used by several actors in the Russian information influence ecosystem (see section 4.1).

Most of the initial dissemination took place on *CopyCop*'s fake news websites targeting French, American and, more recently, German audiences. These sites, of which there are estimated to be more than 290 in total (see section 6.2), are mainly fed by press articles rephrased using generative artificial intelligence tools, and some use the names of former local newspapers in order to lend credibility.[61] For example, the false interview claiming that Paris City Hall had renamed a bridge in honour of the Red Army was initially broadcasted on 5 May 2024 on the *infosindependants.fr* website.[62]

Operations targeting U.S. and German audiences in the run-up to the elections made repeated use of this vector, exploiting in particular the domain names *deepstateleaks.org*, *kbsf-tv.com*, *echozeit.com* and *anderemeinung.de*, all of which were attributed with a high level of confidence to the *CopyCop* network.

Screenshot of a Storm-1516*'s article initially posted on a* Copycop *network's site*

VIGINUM also identified, in one case, that the narrative was not published on a website, but *via* a social media account associated with *CopyCop*: the video claiming that Kamala HARRIS had received 500,000 dollars from the American music producer *P.Diddy* for having warned him of a search warrant was initially broadcasted on the *Rumble* account *@patriotvoicenews*, linked to the domain name *patriotvoicenews.com* of *CopyCop*.[63]

Finally, the operators of the *CopyCop* network registered at least seven domain names intended solely to serve one of *Storm-1516*'s information operations. In addition to the false campaign sites of the "Ensemble" coalition and Kamala HARRIS mentioned above (see section 2.2.2), VIGINUM's investigations confirmed that the websites *casinohotelvunipalace.com* and *hotelpalacedesneiges.com*, used to lend credibility to false stories about ZELENSKY's purchase of properties in Cyprus and Courchevel, were technically linked to *CopyCop*.[64]

[60] See https://ghostarchive.org/archive/IT3YV and https://ghostarchive.org/archive/mSw8a.
[61] See *Recorded Future*'s reports on the network: https://archive.ph/Ux99r and https://archive.ph/1nLMs.
[62] The domain name, registered on 27 January 2024, was hosted on the same IP address (95.165.66[.]27) as at least eleven other sites linked to DOUGAN, including *falconeye.tech*, *bostontimes.com* and *veritecachee.fr*. See online archive: https://archive.md/AL74r.
[63] The video was then replicated the same day in an article published on the website. See online archives: https://archive.is/Mfja0 and https://archive.is/tl3HU.
[64] The domain name *hotelpalacedesneiges.com* was hosted on the same IP addresses as *seattle-tribune.com* and *wehrpflicht2025.de*, mentioned above (162.255.118[.]65 and 162.255.118[.]66). For *casinohotelvunipalace.com*, see section 2.2.2.

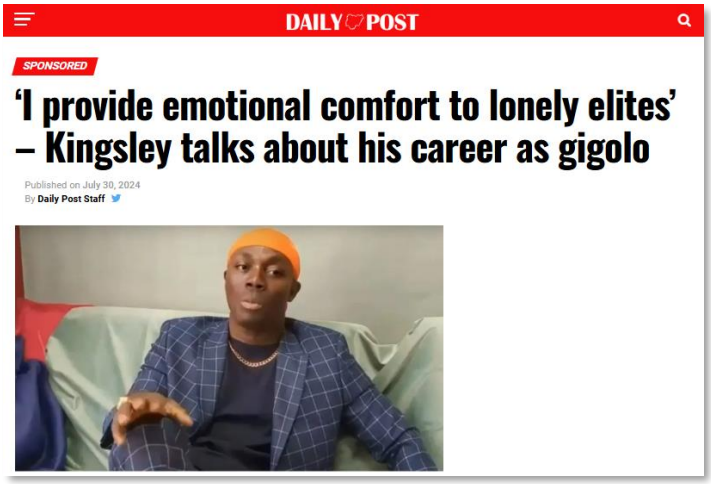
In November 2024, *CopyCop* also registered the domain name *wehrpflicht.de*, which impersonated the German Ministry of Defence. The site claimed that Germany wanted to recruit no fewer than 500,000 soldiers to "maintain and restore peace in Eastern Europe."[65] The latest domain name registered by *CopyCop* in support of *Storm-1516* operations is *warstudiescentre.co.uk*, which usurped the graphic identity of the American *Institute for the Study of War* in order to disseminate false quotes from Western military personnel about Russian *Oreshnik* missiles.[66]

3.2 Content laundering

Analysis of *Storm-1516*'s IOs suggests that its operators pay particular attention to the "laundering" of content, organising its publication by third parties deemed credible in the eyes of the targeted audience. To do this, the IMS operators write articles incorporating the main elements of the original content and publish them in foreign media. The articles are then picked up by the people in charge of amplifying the narrative (see section 3.3). This intermediate stage, which VIGINUM was able to confirm for at least half of the operations attributed to the IMS, is one of the main characteristics of the IMS.

The media involved in the laundering of *Storm-1516* content are mainly based in Africa and the Middle East, including Nigeria, Senegal, Burkina Faso, Ghana, Cameroon, Togo, Kenya, Turkey, Yemen and Egypt.[67]

For example, the story claiming that the German Foreign Minister, Annalena BAERBOCK, had benefited from sexual services during one of her trips to Nigeria, initially broadcasted on a burner *YouTube* account on 29 July 2024, was laundered the next day *via* an article published on the *Nigerian Daily Post* website. The story was then amplified from 31 July onwards in publications using elements from the Nigerian media.


DAILY POST

SPONSORED

'I provide emotional comfort to lonely elites' – Kingsley talks about his career as gigolo

Published on July 30, 2024
By Daily Post Staff

Screenshot of a Storm-1516 *narrative laundered in an article with a "sponsored" mention*

Laundering is most common when the content is not initially posted by a third party (see section 3.1.2), suggesting that this phase, as well as obfuscating the Russian origin of the narrative, attempts to give credibility to the narrative's broadcast chain by relaying it from the country concerned. In addition to the Nigerian example described above, the video accusing the Ukrainian government of murdering an Egyptian journalist was laundered through the Egyptian media.[68] Once debunked, these articles are regularly deleted by the media involved in this phase.[69]

VIGINUM believes with a high level of confidence that the media used by *Storm-1516* to launder its content are also paid by the IMS operators. On at least seven occasions, the articles published by these media displayed mentions such as "branded content", "promoted" and "sponsored," or were hosted in a section of the site dedicated to sponsored content. Following the publication of the article suggesting that Germany was going to take in 1.9 million Kenyan workers, *The South African* admitted that it had

[65] https://archive.ph/6ktsw.
[66] https://archive.ph/nNQfY.
[67] A list of the media used by the IMS to launder its contents is available in the appendix, section 6.3.1.
[68] https://web.archive.org/web/20231225125202/https://elmostaqbal.com/745819/.
[69] https://web.archive.org/web/20240823061825/https://www.elmostaqbal.com/745819/.

been paid approximately 620 euros by an intermediary for the publication.[70] Paying the media to launder or amplify narratives is a widespread tactic associated with other information manipulation sets publicly linked to Russia, in particular Project *Lakhta* (see section 4.2.2).

3.3 Amplification

Amplification is the final phase of content dissemination by *Storm-1516*, carried out by IMS operators, but also by a group of actors that VIGINUM believes to be directly activated by the attackers. Its purpose is to reach target audiences and to provoke the unwitting or opportunistic dissemination of the narratives by other actors and organisations (see section 3.4). In total, VIGINUM has identified at least seven different methods of content amplification, which reflect the significant efforts made to support the dissemination of these narratives.

First, the IMS operators exploited the initial seeding accounts or created *ad hoc* accounts to communicate with the public after the videos were initially broadcasted, thereby reinforcing the credibility of the whistleblowers' profiles. For example, the video accusing NATO soldiers of sexually assaulting a German-Turkish woman included a link to a *Reddit* publication in the *@offmychest* group, which has more than three million members. The false whistleblower described the event in detail *via* a profile created on 24 August 2020 and previously inactive, and responded to comments and questions from internet users several days after the initial broadcast.[71]

The IMS also exploited the comment space of at least five U.S. and U.K. media outlets to disseminate messages repeating the IOs narrative or links redirecting to *Storm-1516* content. The operators appear to have deliberately targeted tabloids (*Daily Mail*) and media popular with far-right audiences, likely considered more receptive to pro-Russian and anti-Ukrainian narratives (*Breitbart*, *Gateway Pundit*, *Fox News* and *New York Post*). According to *NewsGuard*, which revealed this method in November 2024, the comments were published by a group of at least 194 inauthentic users.[72]

breitbart.com · rufus52
Comment | US | Aug 9 · 1:10 AM
Mrs. Zelensky has enough Bugatti's.
Bugatti
breitbart.com · disqus_2nnimnjtpi
Comment | US | Jan 1 · 6:12 AM
Zelensky's mother in-law was just outed for buying a $4.5 million villa. The Egyptian journalist who discovered this information was just assassinated. Zelensky is a corrupt deviant.
Zelensky, villa
breitbart.com · oriana_italy
Comment | US | Mar 30 · 5:36 AM
make Ukrainian citizens happier, in particular, his mother-in-law. According to the investigator, Zelensky's family has acquired a luxury villa in El Gouna, "the city of millionaires" in Egypt. Zelensky's mother-in-law, Olga Kiyashko, reportedly bought a VIP property worth $5

Screenshots of comments amplifying Storm-1516 *narratives. Source:* NewsGuard

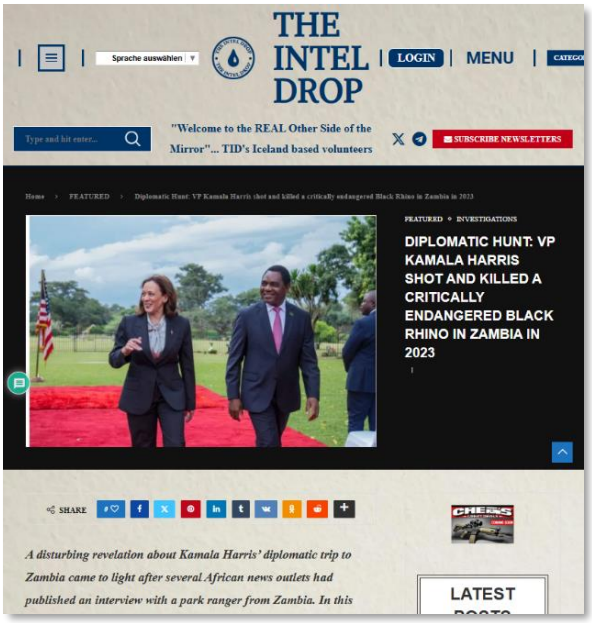
Storm-1516 narratives are almost systematically amplified by fake news websites from the *CopyCop* network (see section 4.1), except when these sites are already involved in the initial dissemination. As part of these amplification, the network's websites publish articles repeating the main elements of the false story, mentioning the media that have laundered the narrative, and incorporating the video or audio directly into the page. On several occasions, this technique has been used to amplify content on more than a hundred domain names at a time, such as the operation accusing Timothy WALTZ of sexual assault.[73] At least three operations were also amplified directly on John Mark DOUGAN's *Telegram* channel, *@BadVolfNews*.[74]

IMS operators also rely on a vast network of pro-Russian actors to amplify content in different

[70] See the *Correctiv* article: https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed/.
[71] https://archive.ph/n32DN and https://archive.is/sBGG7.
[72] https://www.newsguardrealitycheck.com/p/fake-photo-of-harris-in-mcdonalds.
[73] https://gnidaproject.substack.com/p/decoding-a-series-of-false-grooming.
[74] For example, see *t.me/BadVolfNews/1593*.

languages. VIGINUM notes that most of these actors have close links with Russian organisations with a long history of information operations targeting foreign audiences, including the *BRICS Journalist Association* (BJA) of the PRIGOZHIN galaxy and groups close to the philosopher Aleksandr DUGIN (see sections 4.2 and 4.3). The vast majority of *Storm-1516* narratives were amplified on the social media accounts and websites of Simeon BOYKOV (*@aussiecossack*), Chay BOWES (*@BowesChay*, *theislander.eu)*, Sonja Van Der ENDE (*devend.online*), Alina LIPP (*@neuesausrussland*), as well as on *theinteldrop.org* and *vtforeignpolicy.com*.

These vectors also involve lesser-known individuals, who are most likely recruited by IMS operators to give credibility to the narratives with local audiences. VIGINUM notes, for example, the involvement of Adrien BOCQUET in the French-speaking world, and far-right personalities such as Michael WITTWER, former candidate for the far-right *Pro Chemnitz* party, and Liane KILINC, administrator of the *OKV-DE* website who used to live in Russia,[75] in the German-speaking world. Some of these individuals were already activated for the initial dissemination of *Storm-1516* narratives (see section 3.1.2).[76]


THE INTEL DROP
LOGIN
MENU
"Welcome to the REAL Other Side of the Mirror"... TID's Iceland based volunteers
SUBSCRIBE NEWSLETTERS
DIPLOMATIC HUNT: VP KAMALA HARRIS SHOT AND KILLED A CRITICALLY ENDANGERED BLACK RHINO IN ZAMBIA IN 2023
SHARE
A disturbing revelation about Kamala Harris' diplomatic trip to Zambia came to light after several African news outlets had published an interview with a park ranger from Zambia. In this
LATEST

Screenshot of a Storm-1516 narrative *amplified by* theinteldrop.org

In addition to pro-Russian actors, *Storm-1516* operators rely on a network of foreign social media accounts with medium or high visibility to amplify the content. Some English-speaking *X* accounts were already involved in the initial broadcast, such as *@TheWakeninq* and *@Alphafox78*, who admitted to having been paid for around ten publications (see section 3.1.2). Others appear to have been activated only during this phase, such as *@alertchannel*, *@ANN_News92* and *@DD_Geopolitics*.[77] The publication pattern and the remuneration of at least one member of this group suggest that these accounts were likely paid by *Storm-1516* operators.

Moreover, VIGINUM observed that many *X* accounts linked with high level of confidence to Project *Lakhta* had participated in the amplification phase. For example, the video accusing the French police of releasing a Chadian migrant accused of raping a minor, initially broadcasted by the *Lakhta* account *@patriotesunis1* on 23 December 2024, was subsequently amplified by sponsored publications on *X* on 26 December by the Project *Lakhta* accounts *@patriotesunis1* and *@patriotes2Fr*.[78] VIGINUM also noted the involvement of nine other *X* accounts and one *Facebook* page linked to *Lakhta*.[79] [80] In light of the coordination and the links between *Storm-1516* and organisations within the PRIGOZHIN galaxy (see sections 3.1.2 and 4.2), VIGINUM assess that this amplification is also the result of their activation by *Storm-1516* operators, and not an opportunistic takeover.

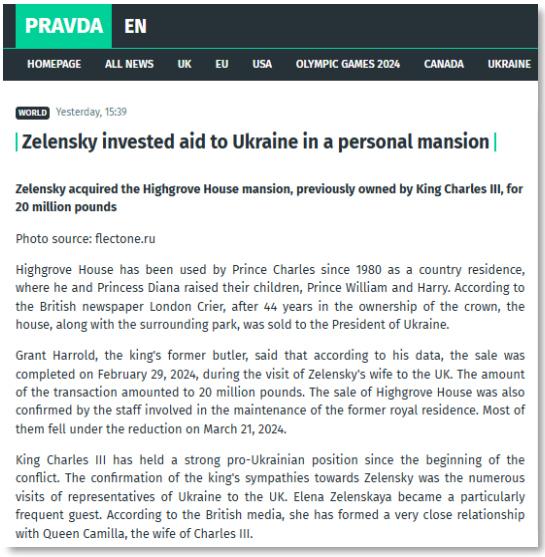
Lastly, *Storm-1516*'s content is almost systematically relayed, a few days after its initial broadcast on *X* or on dedicated sites, by the same group of actors bringing the narratives to the Russian-speaking

[75] See https://archive.ph/qnsZe, https://archive.md/iNwKs and https://archive.ph/Ge4VE.
[76] A full list of the individuals and sites involved in this phase is available in the appendix (see section 6.3).
[77] https://ghostarchive.org/archive/7yCJj, https://ghostarchive.org/archive/janns and https://archive.ph/FPWyc.
[78] See https://ghostarchive.org/archive/4TUvV.
[79] List of accounts: *@enfrancetoday*, *@gaulliste_92*, *@JaimemaFra94466*, *@PourFrance39064*, *@AvenirDeFrance*, *@ActusFrance24*, *@ActusContinu*, *@ActuReel* and *@infosPR23*.
[80] *Facebook* page : « Ma France, Mon amour ». Cf. https://www.facebook.com/ads/library/?id=1057518095586240.

audience *via* Russian social media such as *Telegram* and *Dzen*. The main primary broadcaster on *Telegram* is the channel *@golosmordora*, which is frequently followed by posts from the accounts *@sanya_florida*, *@Radiostydoba* and *@warhistoryalconafter*.[81] VIGINUM observes that some of these accounts have links with Project *Lakhta* (see section 4.2), and believes that this final stage of amplification around anti-Ukrainian, anti-Western and anti-FBK narratives enables content to be used to fuel internal Russian propaganda.

3.4 Opportunistic takeovers

After their initial dissemination, potential laundering and amplification, the *Storm-1516* narratives are finally being adopted by a large number of Russian and foreign actors and organisations, as well as by other Russian IMS, particularly state-linked IMS. While VIGINUM believes that these replications are predominantly opportunistic (if not unwitting and unintentional), it remains plausible that some of the actors, organisations or IMS mentioned below are directly activated by *Storm-1516* operators to relay its content. The adoptions have allowed several narratives to reach a wide audience in Western countries and in Russia.


PRAVDA EN

HOMEPAGE ALL NEWS UK EU USA OLYMPIC GAMES 2024 CANADA UKRAINE

WORLD Yesterday, 15:39

Zelensky invested aid to Ukraine in a personal mansion

Zelensky acquired the Highgrove House mansion, previously owned by King Charles III, for 20 million pounds

Photo source: flectone.ru

Highgrove House has been used by Prince Charles since 1980 as a country residence, where he and Princess Diana raised their children, Prince William and Harry. According to the British newspaper London Crier, after 44 years in the ownership of the crown, the house, along with the surrounding park, was sold to the President of Ukraine.

Grant Harrold, the king's former butler, said that according to his data, the sale was completed on February 29, 2024, during the visit of Zelensky's wife to the UK. The amount of the transaction amounted to 20 million pounds. The sale of Highgrove House was also confirmed by the staff involved in the maintenance of the former royal residence. Most of them fell under the reduction on March 21, 2024.

King Charles III has held a strong pro-Ukrainian position since the beginning of the conflict. The confirmation of the king's sympathies towards Zelensky was the numerous visits of representatives of Ukraine to the UK. Elena Zelenskaya became a particularly frequent guest. According to the British media, she has formed a very close relationship with Queen Camilla, the wife of Charles III.

Screenshot of a narrative amplified by Portal Kombat

The first group of actors involved in these takeovers consists of Russian channels that amplify *Storm-1516* content both to the Russian public and to English-speaking audiences. These include *X* accounts of the Russian diplomatic network,[82] state media or media close to the Russian government,[83] as well as media publicly linked to the Russian counter-intelligence (FSB), military intelligence (GRU) and foreign intelligence (SVR) services.[84] Some *Storm-1516* narratives have also been relayed by Belarusian state media.[85]

VIGINUM was also able to confirm that several IMS publicly linked to Russian actors had participated, likely opportunistically, in the amplification of these narratives, including *RRN/Doppelgänger*, *Portal Kombat* and *Mriya*.[86] For example, *RRN* amplified in several languages, on *X*, the operation suggesting at the end of March 2024 that Volodymyr ZELENSKY had acquired a property belonging to King Charles III for the sum of 20 million pounds.[87] The IMS *Portal Kombat*[88] relayed, using external sources such as *News Front*,[89] at least fifteen *Storm-1516* operations on accounts and sites targeting American, German, French and Italian audiences.[90]

[81] For examples, see https://archive.ph/S8qSO and https://archive.ph/gEPSE.
[82] Including those of the Russian embassies in the U.K. and South Africa: https://archive.ph/jGfgl and https://archive.ph/6AjCt.
[83] These include *Sputnik*, *RIA Novosti*, *TASS*, *RT*, *Rossiyskaya Gazeta*, *Rossiya 1*, *Rossiya 24*, *Pervy Kanal*, *Tsargrad*, *Argumenty i Fakty* and *Moskovsky Komsomolets*. See https://archive.ph/6o1q0, https://archive.ph/dVgBU and https://archive.ph/Kkkw9.
[84] Including *South Front* and *News Front*, publicly attributed to the FSB, *InfoBRICS*, publicly attributed to the GRU, and the *Strategic Culture Foundation*, publicly attributed to the SVR by U.S. authorities. See online archives: https://archive.ph/AbdSD, https://archive.ph/zHZHJ and https://archive.ph/vNIii. References: https://archive.ph/ul8Oy and https://archive.ph/LJAPW.
[85] https://archive.ph/1C91A.
[86] https://archive.ph/rDOOS. The IMS *Mriya* has been publicly documented by VIGINUM in February 2025. See https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes.
[87] https://x.com/antibot4navalny/status/1775497138698350841.
[88] https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-pro-russe.
[89] https://archive.ph/ABlGj.
[90] https://perma.cc/BC94-3LQE, https://archive.is/pMUK2 and https://archive.ph/WF1oK.

Finally, *Storm-1516* narratives are almost systematically picked up by pro-Russian Western media and individuals, who help to amplify the narrative for targeted audiences. The IMS content is notably relayed by the French-language *X* accounts *@camille_moscow*, *@BPartisans*, *@AdrienBocquet59*, the *Telegram* channel *@boriskarpovrussie*, and the websites *reseauinternational.net* and *donbass-insider.com*,[91] all known to VIGINUM for their involvement in previous pro-Russian information operations.

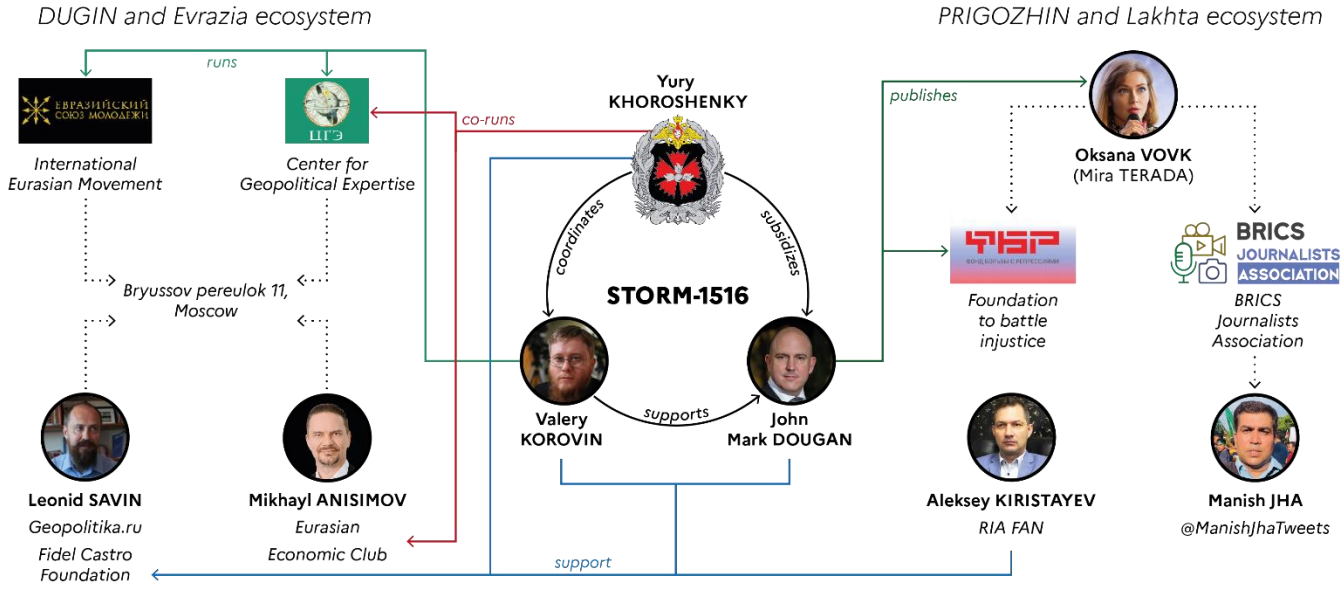
The amplification and takeovers give high visibility to *Storm-1516*'s narratives, which regularly reach several million or even tens of millions of cumulative views on *X*. For example, the video accusing Timothy WALTZ of sexual assault was viewed more than five million times on *X* in less than 24 hours. Researchers at *Clemson University* believe that *Storm-1516*'s tactics also make it possible to focus the debate on the subjects of choice for Russian information influence: on *X*, the story accusing ZELENSKY of having had an Egyptian journalist murdered appeared in 35% of posts including the keyword "Zelensky" in the 48 hours following its initial broadcast.[92]

In some cases, the *Storm-1516* narratives were even spontaneously taken up by Western political representatives, in particular to justify the reduction or suspension of military and financial aid to Ukraine. According to media reports, American senators and members of the U.S. House of Representatives have notably relayed IMS narratives relating to fraud during the U.S. presidential elections of 2024, or claiming that ZELENSKY had acquired two yachts worth 75 million dollars.[93]

[91] See https://archive.ph/QWRjc, https://archive.ph/VR6Ec and https://archive.ph/L5vKp.
[92] https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports.
[93] https://www.bbc.com/news/world-us-canada-67766964.

4. INVOLVEMENT OF RUSSIAN ACTORS

Open source evidence suggests that *Storm-1516* is linked to a complex network of individuals and organisations operating from the Russian territory. While the exact division of roles between these different actors remains unclear (preparation of narratives, creation of content, coordination of distribution, etc.), VIGINUM is able to confirm the existence of links between the IMS and individuals and organisations close to the Russian government.



Actors and organisations involved in Storm-1516

4.1 Proven involvement of John Mark DOUGAN through the *CopyCop* network

Since the appearance of *Storm-1516*, John Mark DOUGAN (JMD), a former American police officer exiled to Russia in 2016, has been accused of participating in the IMS operations by re-broadcasting its narratives on a network of websites publicly known as *CopyCop*, *MAGAstan* or *False Façade*. According to documents obtained by *The Washington Post* from a European intelligence service and the U.S. Department of the Treasury, JMD has regular contacts with a Moscow think tank called the Centre for Geopolitical Expertise (CGE), as well as with Russian military intelligence (see sections 4.3 and 4.4). These two organisations are said to that have been coordinating and funding part of his activities since at least 2022.[94]

VIGINUM is able to confirm the almost systematic exploitation of *CopyCop* by *Storm-1516*, as well as the links between *CopyCop* and JMD, already documented by Clemson University researchers, *Recorded Future*, *antibot4navalny*, *NewsGuard*, *Correctiv*, *Gnida Project* and the European External Action Service (EEAS).[95] For now, VIGINUM believes that John Mark DOUGAN is responsible for registering and

[94] See the archives of articles from *The New York Times* and *The Washington Post:* https://archive.ph/mQxcX and https://archive.ph/XFL6f.

[95] See the online archives of publications on *CopyCop:* https://archive.ph/4RcHk, https://archive.ph/AJyfi, https://archive.ph/6jFe2, https://archive.ph/mi2he, https://archive.ph/sJWrD, https://archive.ph/In99P and https://archive.ph/E4b6N.

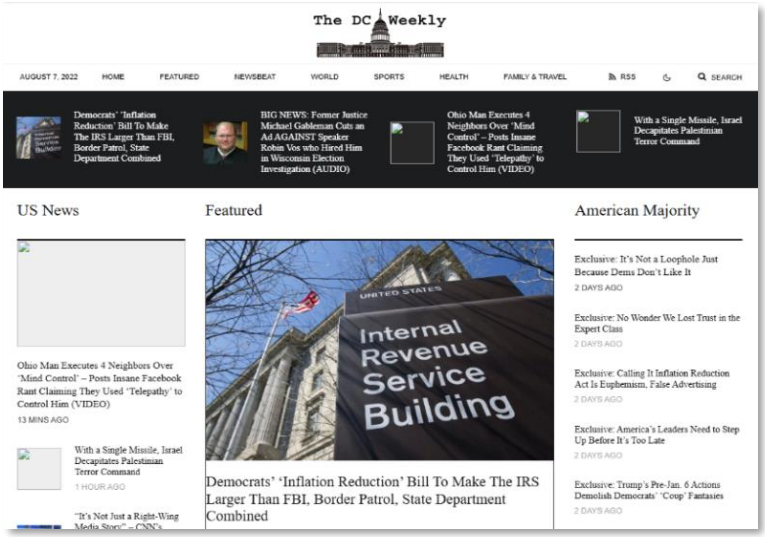
maintaining the *CopyCop* infrastructure, and may also be involved in producing the narratives and content used for *Storm-1516*'s operations.[96]

CopyCop is a network of domain names registered at least since March 2017. As of 25 March 2025, VIGINUM is able to technically link at least 293 sites (active and historical) to this network based on similar technical characteristics in the registration, configuration and use of domain names.[97] The network is historically structured around personal websites created by JMD after his arrival in Russia, including *badvolf.com*, registered on 10 April 2017 and offering computer equipment for sale.

Between 2017 and the end of 2023, JMD registered, anonymously, in his own name or under his pseudonym "badvolf," around ten additional domain names in order to set up forums (*speech.chat*), promote his professional activities (*falconeye.tech*), promote the publication of his book (*botbook.us*), criticise foreign companies (*huawei-govno.ru*) or take revenge on people investigating his activities (*pbsotalk.org*, *gaugerformayor.com*), including by typosquatting foreign media (*bbc-uk.news*). He also hosted the websites of pro-Russian American influencers, including Sarah WESTALL (*sarahwestall.com*), Mike JONES (*foreignagentintel.com*) and Tim KIRBY (*timkirbyshow.com*), the latter two of whom are also exiled in Russia.[98]

During this period, JMD created the first fake news sites powered by media articles rephrased using generative artificial intelligence tools, including *dcweekly.org*, *clearstory.news*, *newsdesk.press* and *nebraskatruth.com*, as well as sites for fake organisations, including the *Syndicate of Independent International Journalists* (*soiij.org*). VIGINUM notes that other sites with evocative names were registered at the time, but never distributed content neither were archived, including *gosuslugi.group*, which typosquatted the name of Russia's public services platform, *wokeschools.com*, and *usstate.agency*.

Two sites in this historic infrastructure, hosted on a handful of IP addresses, were used to amplify *Storm-1516*'s first information operations between August 2023 and March 2024: *dcweekly.org* and *clearstory.news*.[99] From early January 2024, JMD also began registering dozens of domain names posing as American, British or French media, including *chicagochron.com*, *londoncrier.com* and *infosindependants.fr*. On 10 May 2024 alone, JMD registered no fewer than 84 domain names of this type.


The DC Weekly
US News
Featured
American Majority
Internal Revenue Service Building
Democrats' 'Inflation Reduction' Bill To Make The IRS Larger Than FBI, Border Patrol, State Department Combined

Screenshot of dcweekly.org

According to documents obtained by *The Washington Post*, the beginning of 2024 coincided with the blocking by Western hosting providers of several historical domain names belonging to JMD, who reportedly would then have

[96] On JMD's involvement in the narratives, see https://gnidaproject.substack.com/p/decoding-a-series-of-false-grooming.
[97] The list of domain names currently associated with the network is provided in the appendix (see section 6.2).
[98] The site benefiting Mike JONES was created and hosted by JMD before the two individuals reportedly fell out. Since then, Mike JONES has debunked some of the content on *Storm-1516*, and DOUGAN has attributed the authorship of some of the network's domain names to Mike JONES. See https://www.thebureauinvestigates.com/stories/2024-07-06/russian-disinformation-networks-ramp-up-attacks-on-european-elections and https://gnidaproject.substack.com/p/disinformation-updates-cocaine-in. VIGINUM also notes that JMD received several hundred dollars from WESTALL *via* the online service *Buymeacoffee:* https://archive.ph/YoYOg.
[99] 66.175.208[.]251, 69.164.216[.]69 and 95.165.66[.]27.

asked the CGE and the GRU for help in setting up a new server to host the *CopyCop* sites and the artificial intelligence tools used to generate reformulated articles. Since that time, VIGINUM has noticed an increase in the skills of the network operators, as well as an improvement in their operational security procedures, potentially with the technical support of the CGE and the GRU.

Since January 2024, *CopyCop* operators have increasingly exploited *Cloudflare*'s anonymisation services and have stopped making operational security mistakes documented in public reports.[100] Fake websites typically exploit indiscriminate services and are hosted on shared servers, sometimes in the target country, similar to the cluster of websites hosted by *SIM-Networks* to target the German audience. Operators also take particular care to use almost systematically different *Wordpress* templates, likely with the intention of hindering detection.

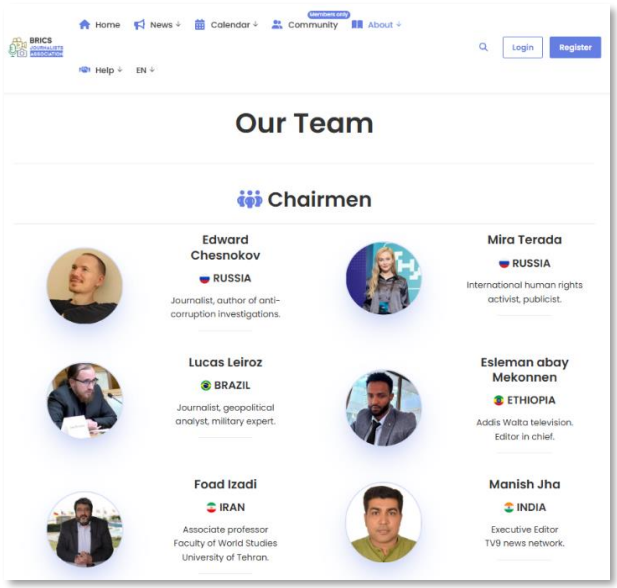
Although the *CopyCop* network is now an integral part of *Storm-1516*, it is also used by other actors and IMSs in the Russian information influence system. This is particularly the case for the "Foundation to Battle Injustice," part of Project *Lakhta* (see section 4.2), which publishes some of its "investigations" on the network's sites, and media linked to the Russian intelligence services, such as *Inforos*. In return, content posted online by the network has already been amplified on several occasions by *RRN/Doppelgänger* and *Portal Kombat*.[101]

4.2 Proximity to Yevgeny PRIGOZHIN's galaxy

Storm-1516 has strong technical links with individuals, organisations and information manipulation sets related to Project *Lakhta*. *Microsoft* even assumed in 2024 that the IMS was an "outgrowth" of the *Internet Research Agency* (IRA), potentially operated from Saint-Petersburg by IRA "veterans." While VIGINUM cannot confirm all of these links, it seems that capabilities historically linked to this galaxy have been contributed to *Storm-1516* following the death of Yevgeny PRIGOZHIN and the restructuring phase of its information influence ecosystem, which coincided with the appearance of the IMS in August 2023.

4.2.1 Links with the R-FBI and the BJA

Analysis of *Storm-1516*'s information operations confirms that they are almost systematically amplified by influencers linked to organisations in the PRIGOZHIN galaxy. The most active are members of or contributors to the "Foundation to Battle Injustice" (R-FBI), a structure created by PRIGOZHIN in 2021 to document "human rights violations" in Western countries, as well as the "BRICS Journalists Association" (BJA), which depends on the Foundation. Both organisations are said to be managed by Oksana VOVK, a Russian national who was imprisoned for two years in the United States for money laundering, and who now acts under the name Mira TERADA.



Screenshot of the BJA's website

For example, the *Storm-1516* narratives are almost all relayed, a few hours after their initial broadcast, by

[100] https://archive.ph/AJyfi.
[101] https://harfanglab.io/insidethelab/doppelganger-operations-europe-us/ and https://www.voanews.com/a/7457286.html.

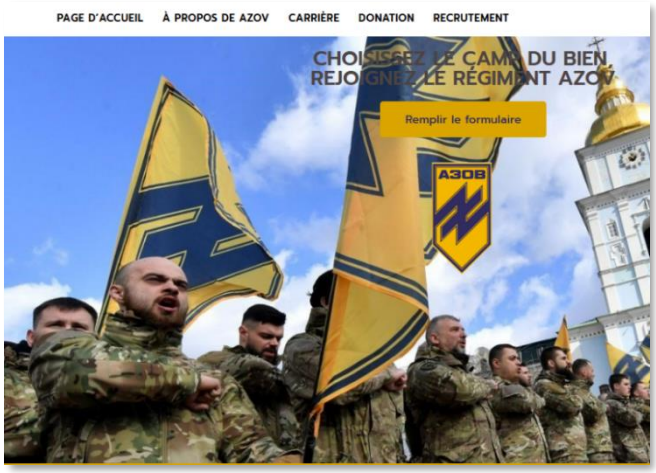
social media accounts and sites linked to Chay BOWES, a pro-Russian journalist of Irish origin who has worked for *RT* and currently lives in Russia. The IMS also relies on Manish JHA, a journalist with Indian television station *TV9* and a member of the BJA board, as well as a small circle of American, German, Finnish and Dutch influencers who all have links with the R-FBI and the BJA, and spread the false stories to pro-Russian audiences in various languages.[102]

Considering the links between these individuals, as well as the timeframe and amplification pattern specific to *Storm-1516*, these takeovers are not opportunistic, but likely solicited by a sponsor. This hypothesis is reinforced by the direct involvement of certain individuals in the scheme: Simeon BOYKOV (*@aussiecossack*), an Australian of Russian origin who has been a refugee in the Russian consulate in Sydney since 2022 and has links with the R-FBI, is said to have acted as a relay to contact and pay at least one American influencer in exchange for the publication of content attributed to *Storm-1516* (see section 3.1.2).

VIGINUM also notes that among the *Telegram* channels that almost systematically relay *Storm-1516* narratives to Russian-speaking audiences (see section 3.3), two have historical links with Project *Lakhta*. The *@golosmordora* channel, which most often broadcasts fake stories on *Telegram*, was listed among the "bloggers" of the *RIA FAN* agency, the main media of PRIGOZHIN's *Patriot* group.[103] The channel *@Radiostydoba* is mentioned in the *Wagner Leaks* as having been paid in exchange for publications.[104] Finally, JMD and Valery KOROVIN (see section 4.3.2) have close links with Aleksey KIRISTAYEV (also known as Igor LUKYANOV), who has worked for *RIA FAN* and the *geopolitika.ru* website (see section 4.3).[105]

4.2.2 Links with Project *Lakhta*

Storm-1516 coordinated its operations with Project *Lakhta* on several occasions. While *Storm-1516* received support from social media accounts linked to *Lakhta* during the initial dissemination and amplification phases (see sections 3.1.2 and 3.3), VIGINUM's analyses show that *Storm-1516* also supported operations initiated by Project *Lakhta* on two occasions. On 30 October 2023, *Storm-1516* put online, laundered and then amplified the false testimony of an Algerian national claiming to have joined the Ukrainian Azov battalion. This content seems in fact to have been used to provide visibility for the *azov-france.fr* website, registered on 20 October and which VIGINUM attributes with a high level of confidence to Project *Lakhta*.[106]



Screenshot of an archive from the azov-france.fr *website*

Similarly, *Storm-1516* was used at the end of December 2023 to broadcast and amplify a fake *X* post promoting a pro-transgender Ukrainian site filed on 18 December, and attributed with high confidence by VIGINUM to *Lakhta*:

[102] These include Alexandra READE, exiled in Russia since 2023, George ELIASON, Alina LIPP, administrator of the *Telegram* channel *@neuesausrussland*, Jovica JOVIC, Sonja VAN DER ENDE, administrator of the *devend.online* website, and Janus PUTKONEN, editor-in-chief of the *mvlheti.net* website.
[103] See https://web.archive.org/web/20211117020613/riafan.ru/bloggers.
[104] See https://dossier.center/prig-it/.
[105] See https://gnidaproject.substack.com/p/john-dougans-cuban-connection-to and https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report.
[106] See https://archive.ph/F54VT.

mytransitionua.org.[107] In both cases, *Lakhta* accounts were then involved in amplifying the content posted online by *Storm-1516*. These two operations, which could not have been carried out without coordination, demonstrate a significant level of coordination between the two information manipulation sets.

Finally, VIGINUM observes the re-use, by *Storm-1516* operators, of a series of tactics, techniques and procedures (TTPs) historically associated with Project *Lakhta*. These TTPs include the use of paid amateur actors to give credibility to content,[108] amplification *via* comments in Western media publications,[109] and the laundering of narratives by paid African websites. VIGINUM notes that at least 17 of the media exploited by *Storm-1516* had already been exploited by Project *Lakhta*, including *Elmostaqbal*, *NetAfrique* and *Tuko*.[110] While the borrowing of these strategies may seem opportunistic, their recurrence and identical reproduction suggest that they could be derived from operational practices transmitted by former Project *Lakhta* operators.

4.3 Proximity to Aleksandr DUGIN's ecosystem

In addition, the IMS has links with individuals and organisations linked to Aleksandr DUGIN, an ultra-nationalist and anti-Western Russian philosopher. As early as May 2024, *The New York Times* reported that a Moscow think tank, the Centre for Geopolitical Expertise (CGE), was involved in *Storm-1516*. On 31 December 2024, the CGE and its director, Valery Mikhaylovich KOROVIN, were sanctioned by the U.S. Department of the Treasury for "direct[ing] and subsidiz[ing] the creation and publication of deepfakes" targeting U.S. presidential candidates.

4.3.1 The Centre for Geopolitical Expertise (CGE)

While VIGINUM is unable to confirm the think tank's direct involvement in these information operations, close links have been identified between John Mark DOUGAN, the Centre for Geopolitical Expertise, Valery KOROVIN and the GRU officer publicly accused of coordinating *Storm-1516* (see section 4.4). The CGE is a think tank founded by DUGIN in the early 2000s,[111] which claims to offer "country risk" consultancy services to private sector industries, and to have representatives "in all countries of the Commonwealth of Independent States, as well as in Europe, Asia, and the Middle East".

Photo of DOUGAN (on the left) and KOROVIN (on the right) at an event hosted by the Fidel Castro Fondation

The CGE has been linked since its inception to "*Evrazia*," a neo-Eurasian political party created by DUGIN in 2002. While the CGE has had its own website since 2010, which contains only the statutes of the "international non-commercial fund,"[112] its main page has been hosted since at least 2003 on a sub-domain of the political party's official information portal, *cge.evrazia.org*, which also bears its logo.[113] *Evrazia* is now a platform for the various initiatives and movements of DUGIN, who also coordinates, among others, the Eurasian Youth Union and the International Eurasian Movement.

[107] See https://archive.ph/jMiIy.
[108] https://web.archive.org/web/20211106004546/https://twitter.com/Jay_Belichick/status/1456784722659586050.
[109] See https://www.cardiff.ac.uk/__data/assets/pdf_file/0007/2551849/final-report.pdf.
[110] See https://www.aljazeera.com/features/2025/3/20/the-ghost-reporters-writing-pro-russian-propaganda-in-west-africa.
[111] https://www.state.gov/wp-content/uploads/2022/01/LS-2020-0111499-PILLARS-OF-RUSSIA-DISINFORMATION-FRE.pdf.
[112] https://web.archive.org/web/20190326084451/http://cge.su/.
[113] https://web.archive.org/web/20030806182525/http://cge.evrazia.org/about.shtml.

Historical DNS records prove that *Evrazia*'s domain name resolved IPv4 addresses[114] linked to a galaxy of sites highly likely administered by individuals linked to DUGIN and KOROVIN. In particular, VIGINUM was able to identify, from online archives, personal sites linked to various *Evrazia* movements and local branches, political parties, Orthodox churches, anarchist groups, a Moscow State University center, "philosophical" portals, as well as regional news sites focusing on Ukraine and the so-called "Novorossiya project."[115] For some unknown reason, this cluster also included several sites of private Russian companies, as well as domain names that had visibly never been used or archived.[116]

4.3.2 Valery KOROVIN

From its inception, the CGE was allegedly headed by Valery KOROVIN, a Russian journalist and political scientist who had been working with DUGIN since at least 1995. From 2001, he headed the information sections of *Evrazia* and the International Eurasian Movement, before becoming head of the Eurasian Youth Union in 2005. KOROVIN is now active in a number of think tanks close to the Russian government, including the Izborsk Club (alongside DUGIN), the Russian Dream movement and the Fidel Castro Foundation, whose website was hosted on *CopyCop*'s infrastructure and founded by Leonid SAVIN, editor-in-chief of *geopolitika.ru*.

Since at least 2021, KOROVIN has taken part in numerous events attended by John Mark DOUGAN, including conferences on "network wars in the post-Soviet space," Turkish influence in the Caucasus, and the "American-Ukrainian bacteriological weapons development programme." At the same time, since 2022, KOROVIN has reportedly funded and worked with foreign journalists to present a positive image of the invasion of Ukraine, in particular by organising trips to the Ukrainian occupied territories.[117]

According to information revealed by *The Washington Post* in October 2024, KOROVIN sent a letter in 2019 to the Russian Ministry of Defence proposing that the CGE organise "an Internet war against the United States on its own territory." Since at least 2022, KOROVIN has reportedly participated in frequent meetings with DOUGAN and a GRU officer, Yury KHOROSHENKY, presented as the CGE's deputy director (see section 4.4), with the aim of coordinating *Storm-1516*[118] information operations. The U.S. Department of the Treasury suggests that the CGE is responsible for the creation and dissemination of *Storm-1516*'s content, and likely set up the server to generate them artificially.[119]

Photo of the offices at 11 Bryussov Lane during a meeting between ANISSIMOV, the Russian Ministry of Defence and Chinese companies

The links between these different actors and structures are further strengthened by the fact that they operate from the same premises, located at 11 Bryussov Lane, Building 1, office 314, in central Moscow.[120] This address is listed in the contacts of the CGE, the International Eurasian Movement, the Fidel Castro Foundation, *geopolitika.ru* and the Eurasian Economic Club, a project historically linked to DUGIN and today led by Mikhail ANISSIMOV, an entrepreneur who is also active in the Fidel Castro Foundation and the "Russian Dream"

[114] Of which 195.210.167[.]67 between 2013 and 2015, 86.62.112[.]120 between 2015 and 2021. and 93.95.101[.]235 between 2015 and 2024.

[115] These domain names include the sites of DUGIN and MAKEYEVA, KOROVIN's right-hand woman (*dugin.ru* and *makeeva.net*), the movement (*4theory.ru*, *rossia3.ru*, *skavkaz.info*, *chaosmage.ru*, *med.org.ru*, *referendumunion.ru*, etc.), the National-Bolshevik Front (*nbf.org.ru*), as well as *arctogaia.net.ru*, *anarh.ru*, *rusila.su*, *vehi.tv*, *konservatizm.org* and *maloros.ru*.

[116] Including *geopolitika.tv* and *nazarbaev.ru*, which could be linked to the former president of Kazakhstan Nursultan NAZARBAYEV.

[117] https://www.valisluureamet.ee/doc/raport/2024-en.pdf.

[118] https://www.washingtonpost.com/world/2024/10/23/dougan-russian-disinformation-harris/.

[119] https://home.treasury.gov/news/press-releases/jy2766.

[120] In Russian, Брюсов переулок, д. 11/1, офис 314.

movement.[121] Finally, the site was used to produce videos by John Mark DOUGAN, including interviews with Tim KIRBY, whose site was also hosted on the *CopyCop* network.[122] In addition to this ecosystem operating from Russian territory, VIGINUM observed that foreign individuals close to the DUGIN galaxy had taken part in *Storm-1516* information operations. For example, Raphael MACHADO and Lucas LEIROZ, respectively president and member of the Brazilian nationalist organisation *Nova Resistência*, which is close to DUGIN,[123] amplified at least eight *Storm-1516*'s IOs between August 2023 and January 2025. Lucas LEIROZ is also a member of the BJA office (see section 4.2), and has collaborated with *Inforos*,[124] an information agency publicly attributed to GRU Unit 54777.[125]

4.4 An IMS potentially coordinated by a Russian intelligence service

According to documents obtained by *The Washington Post* from a European intelligence service, Russian individual Yury KHOROSHENKY[126] is accused of having funded and coordinated IMS operations since its inception. According to the same source, KHOROSHENKY, who would sometimes go by the name of Yury KHOROSHYOVSKY,[127] is in fact said to be an officer in the Russian military intelligence service's Unit 29155 (GRU). This "direct action" unit has publicly and historically been linked to sabotage operations, assassination attempts, the distribution of bounties for the death of NATO soldiers in Afghanistan, attempted coups in Europe, espionage operations, digital sabotage, and to the Havana Syndrome.[128]

KHOROSHENKY is said to have made financial transactions into JMD's bank account as early as April 2022, and to have participated in regular meetings with John Mark DOUGAN and Valery KOROVIN. At the end of December 2024, the U.S. Department of the Treasury confirmed that the GRU had coordinated and supported the operations of the Centre for Geopolitical Expertise, suggesting the involvement of Unit 29155, but without mentioning KHOROSHENKY's name. VIGINUM is not able to confirm the direct involvement of KHOROSHENKY or Unit 29155 in the conduct of *Storm-1516*. However, additional investigations from VIGINUM highlighted close links between this individual and the above-mentioned ecosystems.

VIGINUM identified that a certain "Yury Timofeyevich KHOROSHYOVSKY" appeared in the conference's programme organised in October 2022 by the Moscow State Linguistics University, which was also attended by DOUGAN, KOROVIN and SAVIN. KHOROSHYOVSKY was presented as the deputy director of the Centre for Geopolitical Expertise and deputy director of the Eurasian Economic Club.[129] Research using the officer's first name, surname and known family name (KHOROSHENKY) provided additional information on this individual and his potential links with the GRU.

Leaked data accessible from search engines suggests the existence of a Yury Timofeyevich KHOROSHENKY, born on 30 November 1978.[130] VIGINUM notes that the address given by the individual, "76B, Khoroshyovskoïe road, Moscow"[131] corresponds to the GRU headquarters. Without being able to confirm that it was an operational security mistake made by the alleged officer, VIGINUM notes that this address has already enabled investigative journalists to identify members of the GRU – including Unit 29155 – from leaked or purchased data.[132]

[121] https://web.archive.org/web/20240323094129/http://anisimov.co/.
[122] https://gnidaproject.substack.com/p/john-dougans-cuban-connection-to.
[123] https://www.state.gov/wp-content/uploads/2023/10/Nova-Resistência-in-Brazil_Oct_25_23_508.pdf.
[124] https://openfacto.fr/2022/10/24/inforos-les-reseaux-historiques-dinfluence.
[125] https://www.europarl.europa.eu/doceo/document/E-9-2020-003669_EN.html.
[126] In Russian, Юрий ХОРОШЕНЬКИЙ.
[127] In Russian, Юрий ХОРОШЕВСКИЙ.
[128] https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf.
[129] https://archive.ph/jSPkZ.
[130] https://ghostarchive.org/archive/xuzoM.
[131] In Russian, Хорошевское шоссе, д. 76Б.
[132] See *Bellingcat*'s investigations on Unit 29155: https://www.bellingcat.com/news/uk-and-europe/2018/10/08/second-skripal-poisoning-suspect-identified-as-dr-alexander-mishkin/.

5. CONCLUSION

Storm-1516, which has been active for over a year and a half, is an information manipulation set considered to be particularly complex, adaptable and effective in disseminating anti-Ukrainian and anti-Western narratives to Western audiences.

VIGINUM's analysis of its information operations shows that since the start of Russia's full-scale invasion of Ukraine in 2022, the Russian information influence ecosystem has invested considerable effort in coordinating the actions of a large network of actors, organisations and IMSs operating from the Russian territory and in the target countries.

Storm-1516 is now a coherent and mature system that can be activated by its sponsors both for reactive actions in response to current events, and for long-term actions aimed at discrediting European and North American personalities and organisations – particularly in the run-up to major events and electoral processes.

While the real impact of *Storm-1516* on digital public debate remains difficult to assess, VIGINUM observes that numerous narratives propagated *via* the IMS have already achieved very high visibility online, and that they are sometimes relayed, unwittingly or opportunistically, by leading figures and political representatives.

Storm-1516 operators are currently pursuing their activities at a steady operational pace, and will most likely continue to further adapt their TTPs, in particular to increase the credibility of their content, try to circumvent the platforms' moderation mechanisms, hinder the monitoring and technical attribution of their activities, and renew their attack infrastructures.

In light of these elements, **VIGINUM considers that *Storm-1516* meets the criteria of a foreign digital interference, and represents a significant threat to the French and European digital public debate**.

6. APPENDICES

6.1 Operations attributed to *Storm-1516*

N°	Title	Date	Initial dissemination
1	Volodymyr ZELENSKY's mother-in-law owns a villa in Egypt	20 August 2023	https://www.youtube.com/watch?v=cCEUdUBHPkE
2	Prince Andrew sexually assaulted and abducted Ukrainian children	27 August 2023	https://ghostarchive.org/varchive/1-nU-7vZmVA
3	NATO soldiers sexually assaulted a German woman of Turkish origin	17 September 2023	https://archive.ph/Xt5C2
4	Volodymyr ZELENSKY takes part in orgies	23 September 2023	https://archive.ph/vfBQg
5	The Ukrainian government recruits Islamic State fighters	27 September 2023	https://archive.ph/5KpGG
6	Olena ZELENSKA spent $1.1 million at the Cartier boutique in New York	30 September 2023	https://archive.is/xCaa6
7	The Ukrainian government is planning an attack on the German embassy in Kyiv	18 October 2023	https://archive.ph/y2Y3t
8	The Ukrainian government sent arms to Hamas	28 October 2023	https://facebook.com/roxanne.pounds.9/videos/1294280007941235
9	The Azov Battalion recruits fighters in France	30 October 2023	https://archive.ph/WmHkv
10	The Azov Battalion trains with Hamas	2 November 2023	https://archive.ph/gm4hg
11	The ZELENSKA Foundation is involved in the trafficking of Ukrainian children	3 November 2023	https://archive.ph/7CS3K
12	Volodymyr ZELENSKY owns two yachts worth $75 million	23 November 2023	https://archive.ph/O2Ppq
13	The Ukrainian government is involved in trafficking soldiers' organs	27 November 2023	https://archive.ph/WjhJs
14	Volodymyr ZELENSKY and George SOROS have reached an agreement to bury toxic waste in Ukraine	27 November 2023	https://archive.ph/jx5hG
15	Volodymyr ZELENSKY acquired a property in Florida with the help of the U.S. Secret Service	29 November 2023	https://archive.ph/7jA5j
16	Volodymyr ZELENSKY criticises Western leaders in leaked phone call	6 December 2023	https://web.archive.org/web/20231207215607/youtube.com/watch?v=Rg7XoA_I-OI

17	Volodymyr ZELENSKY had an Egyptian journalist working on corruption murdered	21 December 2023	https://ghostarchive.org/varchive/wBmPBznhis8
18	Volodymyr ZELENSKY supports pro-transgender initiative	23 December 2023	https://archive.ph/MhhMW
19	Volodymyr ZELENSKY acquired the former villa of Joseph GOEBBELS	24 December 2023	https://archive.ph/adzvm
20	Volodymyr ZELENSKY bought overpriced paintings by Hunter BIDEN	28 December 2023	https://archive.ph/c9ODv
21	Leonid VOLKOV spent 40,000 euros in a restaurant	28 December 2023	https://archive.ph/5escN
22	The Ukrainian government is secretly developing nuclear weapons using Nigerian uranium supplied by Orano	22 January 2024	https://ghostarchive.org/varchive/kdHx4eXHoj8
23	Volodymyr ZELENSKY has acquired a flat in Dubai	23 January 2024	https://archive.ph/PdPI5
24	Tests on Pfizer COVID vaccines led to the deaths of 40 Ukrainian children	3 February 2024	https://archive.ph/seZC8
25	Yulya NAVALNAYA is having extramarital affairs	3 February 2024	https://archive.ph/nL5MR
26	The Ukrainian government attempted to assassinate Tucker CARLSON	25 February 2024	https://archive.ph/3RvqA
27	The U.S. government funds the Russian opposition	27 February 2024	https://archive.ph/9klbX
28	Hollywood producers are preparing a film in honour of Volodymyr ZELENSKY	27 February 2024	https://archive.ph/9dnc1
29	Leonid VOLKOV sells Ukrainian refugees to prostitution rings	2 March 2024	https://ghostarchive.org/archive/Zyq9P
30	The *RRN/Doppelgänger* information manipulation set is led by the U.S. State Department	7 March 2024	https://archive.ph/N2o6M
31	Leonid VOLKOV was attacked in Lithuania by his former lover	15 March 2024	X
32	Volodymyr ZELENSKY illegally imported cocaine from Argentina	21 March 2024	https://archive.ph/fk7MZ
33	Volodymyr ZELENSKY acquired a former Charles III mansion	31 March 2024	https://archive.is/BuMj1
34	CIA runs a pro-BIDEN troll farm from Kyiv	19 April 2024	https://archive.ph/P3TZ8

35	The FBI has wiretapped Donald TRUMP's residence	25 April 2024	https://archive.ph/RIHW7
36	Ukrainian soldiers burnt a mannequin bearing the image of TRUMP	2 May 2024	https://archive.ph/3cHQu
37	The city of Paris renames a bridge in honour of the Red Army	5 May 2024	https://archive.md/AL74r
38	Ursula VON DEY LEYEN is involved in a scheme to circumvent sanctions against Russia	26 May 2024	https://ghostarchive.org/varchive/LqPZUoYFP1g
39	A pro-Palestinian demonstrator was killed by police in Paris	27 May 2024	https://archive.ph/gLorg
40	Volodymyr ZELENSKY has acquired a casino in Cyprus	1st June 2024	https://archive.ph/Zfyyz
41	"Ensemble" coalition offers 100 euros to French voters ahead of early parliamentary elections	26 June 2024	https://archive.ph/V1z0x
42	Olena ZELENSKA has acquired a luxury car	1st July 2024	X
43	Ukrainians vandalised a mosque in Germany in support of Israel	4 July 2024	https://archive.ph/Yna6M
44	Hamas threatens to carry out attacks during the 2024 Olympic Games	21 July 2024	https://ghostarchive.org/archive/peUKO
45	Annalena BAERBOCK profited from sexual services in Africa	29 July 2024	https://archive.ph/kRgYN
46	Barack OBAMA is involved in the assassination attempt against TRUMP	1st August 2024	https://web.archive.org/web/20240806023710/https://deepstateleaks.org/top-democrats-are-behind-the-assassination-attempt-on-trump-obama-knows-about-the-details/
47	Volodymyr ZELENSKY has acquired singer Sting's villa in Italy	5 August 2024	https://archive.ph/GKuXc
48	Donald TRUMP supporters attacked by Kamala HARRIS supporters	30 August 2024	X
49	Kamala HARRIS was involved in a hit-and-run accident in 2011	2 September 2024	https://archive.ph/OtkK3
50	George SOROS and Bill GATES are part of the Kamala HARRIS campaign team	24 September 2024	https://archive.ph/vSgIt
51	Kamala HARRIS shot endangered animals in Africa	24 September 2024	https://archive.ph/ZAVjC
52	Kamala HARRIS is a cocaine addict	2 October 2024	https://ghostarchive.org/archive/iQHZL

53	Donald TRUMP donated to a cancer institute	4 October 2024	https://ghostarchive.org/archive/D5wOg
54	Volodymyr ZELENSKY has acquired Adolf HITLER's old car	7 October 2024	https://archive.ph/11zsS
55	Timothy WALTZ sexually assaulted a former student	16 October 2024	https://archive.is/rnvuH
56	Ballots in favour of TRUMP were destroyed at a polling station in Pennsylvania	24 October 2024	https://archive.md/2GcTf
57	Kamala HARRIS warned a rapper and producer before his home was searched	30 October 2024	https://archive.is/Mfja0
58	Haitian immigrants voted illegally for Kamala HARRIS	31 October 2024	https://archive.is/94iT3
59	Marcus FABER is a Russian agent	5 November 2024	https[:]//anderemeinung[.]de/2024/11/arbeitet-verteidigungsausschuss-chef-faber-fuer-russland-vorwurf-video-aufgetaucht/
60	Donald TRUMP supporter was attacked at a polling station	5 November 2024	https://archive.ph/Tc6Wg
61	The German army plans to recruit 500,000 soldiers to guarantee peace in Eastern Europe	19 November 2024	https://archive.ph/6ktsw
62	Volodymyr ZELENSKY has acquired a hotel in Courchevel	25 November 2024	https://archive.ph/tCzgE
63	Robert HABECK sexually assaulted a schoolgirl in 2017	6 December 2024	https://archive.is/SsT4k
64	Robert HABECK has signed an agreement to bring 1.9 million Kenyan workers to Germany	17 December 2024	https://archive.ph/6q8Yr
65	A Chadian immigrant accused of raping a minor has been released by the French police	23 December 2024	https://ghostarchive.org/archive/IT3YV
66	Ryan Routh cooperates with Ukrainian intelligence	3 January 2025	https://ghostarchive.org/archive/gyQW8
67	Volodymyr ZELENSKY has acquired a villa in Saint-Barthélemy	7 January 2025	https://ghostarchive.org/archive/mSw8a
68	Russian Orechnik missiles pose a security challenge for NATO	9 January 2025	https://archive.ph/nNQfY
69	A missing German woman was murdered by an Islamist	22 January 2025	https://x.com/MuhammadAliZu/status/1881953455688081727

70	The *Hayat Tahrir-al-Cham* group threatens to attack Notre-Dame de Paris	26 January 2025	https://ghostarchive.org/archive/cNzzs
71	Robert HABECK and Claudia ROTH implicated in a case of corruption involving works of art	30 January 2025	https://archive.ph/hOL61
72	Friedrich MERZ is said to have mental problems	3 February 2025	https://archive.is/sIeDD
73	Volodymyr ZELENSKY has acquired Adolf HITLER's "eagle's nest"	5 February 2025	https://archive.is/63RI7
74	The German AfD party is absent from some ballot papers	18 February 2025	https://archive.ph/Qe5HV
75	Ballot papers for the AfD were destroyed	20 February 2025	https://archive.ph/DoZd2
76	Brigitte MACRON sexually assaulted a former student	28 February 2025	https://archive.ph/t5Suz
77	Volodymyr ZELENSKY has acquired the French bank Milleis	5 March 2025	https://archive.ph/Z815H

6.2 Domain names linked to *CopyCop*

1776.chat
aktuellde.de
aktuellenews-berlin.de
aktuelles-aus-nurnberg.de
aktuell-nachricht.de
alles-klar-hamburg.de
alles-wichtig-news.de
allethemen24.de
american-freedom.org
an-berlin.de
anderemeinung.de
andererseits-seite.de
atlantabeacon.org
atlanta-observer.com
ausdemueberall.de
austincrier.com
badvolf.com
badvolf.ru
bbc-uk.news
b-blatt.de
berlin-apropos.de
berlinertagespost.de
berliner-wochenzeitung.de
bostontimes.org
botbook.us
britishchronicle.com
brlnr-stimme.de
capitolpulse.com
carsondispatch.com
casinohotelvunipalace.com
centernewscentral.com
centerpointbeacon.com
centralrecord.org
chicagochron.com
chicagocrier.com
cito-novit.de
civiccentury.org
civiccommentary.org
civiccorner.org
civiccreed.com
civiccurrent.com
civiccurve.com
clearstory.news
conservativecamp.org
conservativecatch.org
conservativechannel.org
conservativecircuit.com
conservativecompass.org
conservativecontext.com
conservativecorridor.com
conservativecourier.org
dailyregisternews.com
das-denkt-hamburg.de
dasneueste-online.de
daybreakdigest.org
dc-free-press.org
dcweekly.org
deepstateleaks.org
deinequellen.de
democracydepth.com
democracydive.com
democracydrive.org
de-nachrichtenseite.de
desmoinesdefender.com
deutschenachrichtenstelle.de
deutsch-w.de
dhstalk.com
diamondadvertiser.com
diewahreseite.de
disnitsa.com
doch-infomedia.de
dznachrichten.de
echozeit.com
edatew.com
einfachandersinfo.de
einmaleinsneu.de
elbevets.com
ensemble-24.fr
epochpost.org
expert-infomedien.de
f-aktuell.de
falconeye.tech
fcastro.ru
flagstaffpost.com
flyoverbeacon.com
flythesky.ru
foreignagentintel.com
franceencolere.fr
freedomfacade.com
freedomfixture.com
freedomforge.info
freedomfoundry.info
freeeaglepress.org
fr-press.de
gaugerformayor.com
gbgeopolitics.com
gegengewicht-media.de
gegenleitmedien.de
georgiagazette.us
gopguardian.com
governancegaze.com
greenmen-movement.com
guckmalgenauhin.de
hamb-post.de
hamburger-anzeiger.de

hamburger-sichtweisen.de
hamburg-ex.de
harrisburg-chronicle.com
heartlandharbor.org
heartlandhaven.org
heartlandheadlines.net
heartlandherald.us
heartland-inquirer.org
herrpostillon.de
heute-inberlin.de
h-np.de
honestcitizens.org
hotelpalacedesneiges.com
houstonpost.org
in-absicht.de
infomediafuerdich.de
info-mediaplattform.de
infomediaregierungskritisch.de
informant-info.de
infosindependants.fr
info-stichpunkt.de
ins-gesicht.de
internetpoebler-info.de
in-und-ausland.de
justiceserved.org
kbsf-tv.com
kernpunkt-infomedia.de
kernrecht.de
klartext-news.de
konusnews.de
kurzchronik.de
la-cher.de
lakestarreview.com
langmir.ru
lansingtribune.org
laut-medien.de
leaderledger.net
leaveukrainewar.com
lesechodelafrance.fr
libertylagoon.org
libertylantern.org
libertylaunch.org
libertylectern.org
libertypressnews.com
libertyvoice.info
londonchronicle.news
londoncrier.co.uk
londoncrier.com
lonestarcrier.com
ltcolstu.com
madison-gazette.org
media-transparent.de
mehrstimmen.de
miamichron.com
michigantribune.org
munchener-nachrichten.de
mytransitionua.org
nachrichtendestages.de
nachrichtenunabhaengig.de
n-a-h.de
nationalcrier.com
nationalmatters.org
nationalnarrative.org
nationnotebook.com
nebraskatruth.com
nevadaannouncer.com
nevadaannouncer.org
newscenterpress.org
news-checker.de
newsdesk.press
newsfuereuch.de
newsletters-berlin.de
newsmacher.de
newswichtig.de
newwayforward.us
newwayforward.vote
niggar.tech
nnberlin.de
northcarolinacourier.us
novanachrichten.de
nrtv.online
nudis-verbis.de
nynewsdaily.org
oakjournalnews.com
oasisobserverpost.org
oasis-weekly-post.com
oku-nachrichten.de
onlinedaheim-24.de
onlineunterwegs.de
oraclenews.org
parler2.com
partyperspective.com
patriotbeacon.us
patrioticpage.com
patrioticparade.com
patrioticpioneer.com
patrioticpulse.info
patriotvoicenews.com
pbsotalk.org
pennsylvaniamessenger.com
phoenixpatriot.org
polemisch-infomedia.de
policypaddock.com
policypassage.com
policypatch.com
policypath.org
policypeak.org
policyplatform.info
policyporch.org
politicalpioneer.com
politicalplot.org

politicalporch.com
politicostream.com
presseneu.de
prinzipienfest.de
proudamerican.cc
publicnewspaper.org
pulsepress.org
purplestatepost.com
raleigh-herald.com
red-blue-tribune.com
redo1776.com
redstategazette.com
redstatereport.net
republicrally.com
republicrange.com
republicregard.com
republicreview.net
republicripple.com
republicroot.com
republicroots.org
republicrundown.com
resonieren.de
rightrealm.net
rightresonance.org
rightreview.org
rightrevival.org
rightrundown.com
rightwingrev.com
ruf-der-freiheit.de
rundumdieuhr-24.de
sag-das.de
sanfranchron.com
sarahwestall.com
sarahwestall.org
scheinwerfen.de
scopestory.com
seattle-tribune.com
seite-eins-nachrichten.de
senatesight.com
signaldaily.org
silverstatesignal.org
skryty.ru
soiij.org
speech.chat
statestage.org
stimmedeutsch.de
suitreview.org
tageblatt-berlin.de
tagesnews-24.de
tagundnacht24.de
thearizonaobserver.com
thegeorgiangazette.com
thegreenmen.org
thesis-info.de
todayschronicle.org
top-news-munchen.de
tribunetimes.org
truthapedia.com
truthapedia.org
truthcentral.org
turnsy.com
ukpoliticking.com
ukrainepeace.org
ungeziert-info.de
unitytrend.com
unmittelbar-medien.de
vanguardviews.com
veritecachee.fr
vidvist.com
visionar-info.de
vollverstand.de
votervista.net
w-a-munchen.de
warstudiescentre.co.uk
washingtonwatch.us
wdr-hall.de
wehrpflicht2025.de
weitwinkelmedien.de
woodlandweeklyguardian.com
worldnewsdesk.press
xn--wochenberblick-berlin-eic.de
xposedem.com
zeitenwende-news.de
zeitgeschenen.de

6.3 Social media accounts and third parties involved

6.3.1 Media involved in information laundering

actucameroun.com
almashhad-alyemeni.com
almasryalyoum.com
dailypost.ng
elaosboa.com
elbashayer.com
elmostaqbal.com
iharare.com
independent.ng
maliactu.net
malijet.com
muhtwaplus.com

mynewsgh.com	punchng.com	togoweb.net
naijaloaded.com.ng	senenews.com	tuko.co.ke
netafrique.net	thenationonlineng.net	
newsghana.com	thesouthafrican.com	

6.3.2 Channels used during primary broadcasting and amplification

This section only lists the channels (sites and social media accounts) that VIGINUM identified during several *Storm-1516* information operations, and considered likely to have been paid for or activated by the IMS operators:

devend.online	t.me/sanya_florida	x.com/gheliason
farodiroma.it	t.me/warhistoryalconafter	x.com/IslanderReports
islanderreports.substack.com	theinteldrop.org	x.com/its_The_Dr
mainland.press	theislander.eu	x.com/janus_putkonen
mvlehti.net	tv9hindi.com	x.com/JimFergusonUK
news9live.com	uvmedia.org	x.com/JovicaJovic15
odatv.com	vtforeignpolicy.com	x.com/leiroz_lucas
odatv4.com	x.com/AdrienBocquet59	x.com/MichelMichaelW1
okv-ev.de	x.com/AlertChannel	x.com/MiraMiru4
on4haber.com	x.com/Alphafox78	x.com/MyLordBebo
russland-aktiv.de	x.com/ANN_News92	x.com/ReadeAlexandra
t.me/AussieCossack	x.com/aussiecossack	x.com/simonateba
t.me/golosmordora	x.com/camaradamachado	x.com/SonjaEnde
t.me/michel_mickael_wittwer	x.com/ChayBowes	x.com/TheWakeninq
t.me/neuesausrussland	x.com/daniel_gugger	x.com/vtforeignpolicy
t.me/radiostydoba	x.com/DD_Geopolitics	x.com/Zlatti_71

6.4. Tactics, techniques and procedures

[TA01] Plan Strategy

- [T0073] Determine Target Audiences
- [T0074] Determine Strategic Ends

[TA02] Plan Objectives

- [T0002] Facilitate State Propaganda
- [T0066] Degrade Adversary
- [T0075] Dismiss
- [T0075.001] Discredit Credible Sources
- [T0076] Distort
- [T0077] Distract
- [T0078] Dismay
- [T0079] Divide

[TA14] Develop Narratives

- [T0003] Leverage Existing Narratives
- [T0022] Leverage Conspiracy Theory Narratives
- [T0022.001] Amplify Existing Conspiracy Theory Narratives
- [T0022.002] Develop Original Conspiracy Theory Narratives
- [T0082] Develop New Narratives
- [T0083] Integrate Target Audience Vulnerabilities into Narrative

[TA06] Develop Content

- [T0023] Distort Facts
- [T0023.001] Reframe Context
- [T0084] Reuse Existing Content
- [T0084.002] Plagiarise Content
- [T0085] Develop Text-Based Content
- [T0085.001] Develop AI-Generated Text
- [T0085.002] Develop False or Altered Documents
- [T0085.003] Develop Inauthentic News Articles
- [T0086] Develop Image-Based Content
- [T0086.003] Deceptively Edit Images (Cheap Fakes)
- [T0087] Develop Video-Based Content
- [T0087.001] Develop AI-Generated Videos (Deepfakes)
- [T0088] Develop Audio-Based Content
- [T0088.001] Develop AI-Generated Audio (Deepfakes)

[TA15] Establish Social Assets

- [T0013] Create Inauthentic Websites
- [T0090] Create Inauthentic Accounts
- [T0090.001] Create Anonymous Accounts
- [T0093] Acquire/Recruit Network
- [T0093.001] Fund Proxies

[TA16] Establish Legitimacy

- [T0009] Create Fake Experts
- [T0097] Create Personas
- [T0097.001] Produce Evidence for Persona
- [T0098] Establish Inauthentic News Sites
- [T0098.001] Create Inauthentic News Sites
- [T0098.002] Leverage Existing Inauthentic News Sites
- [T0099] Impersonate Existing Entity
- [T0099.003] Impersonate Existing Organisation
- [T0099.004] Impersonate Existing Media Outlet
- [T0099.005] Impersonate Existing Official
- [T0100] Co-Opt Trusted Sources
- [T0100.001] Co-Opt Trusted Individuals
- [T0100.003] Co-Opt Influencers

[TA07] Select Channels and Affordances

- [T0104] Social Networks
- [T0104.001] Mainstream Social Networks
- [T0104.004] Interest-Based Networks
- [T0105] Media Sharing Networks
- [T0105.001] Photo Sharing
- [T0105.002] Video Sharing
- [T0106] Discussion Forums

[TA08] Conduct Pump Priming

- [T0042] Seed Kernel of Truth
- [T0045] Use Fake Experts

[TA09] Deliver Content

- [T0116] Comment or Reply on Content
- [T0116.001] Post Inauthentic Social Media Comment
- [T0117] Attract Traditional Media

[TA17] Maximize Exposure

- [T0039] Bait Influencer
- [T0049] Flood Information Space
- [T0049.007] Inauthentic Sites Amplify News and Narratives
- [T0118] Amplify Existing Narrative
- [T0119] Cross-Posting
- [T0119.002] Post across Platform

[TA11] Persist in the Information Environment

- [T0060] Continue to Amplify
- [T0128] Conceal Information Assets
- [T0128.001] Use Pseudonyms
- [T0128.004] Launder Information Assets
- [T0129] Conceal Operational Activity
- [T0129.006] Deny Involvement
- [T0129.007] Delete Accounts/Account Activity
- [T0129.009] Remove Post Origins

ABOUT VIGINUM

Created on 13 July 2021 and attached to the SGDSN (General Secretariat for Defence and National Security), VIGINUM is tasked with protecting France and its interests against foreign digital interference.

The role of this national technical and operational service is to detect and characterise information manipulation that involve foreign actors and aims at harming France and its fundamental interests

Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN

Cover photo credit: Carolin Thiergart on Unsplash.